ETSI TS 134 229-1 V15.5.0 (2021-05)

TECHNICAL SPECIFICATION

**Universal Mobile Telecommunications System (UMTS);
LTE;
Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP);
User Equipment (UE) conformance specification;
Part 1: Protocol conformance specification
(3GPP TS 34.229-1 version 15.5.0 Release 15)**

Reference

RTS/TSGR-0534229-1vf50

Keywords

LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document is the first part of a multi-part conformance specification valid for 3GPP Release 5 and later releases.

3GPP TS 34.229-1 (the present document): Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification- current document.

3GPP TS 34.229-2 [5]: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".

3GPP TS 34.229-3 [6]: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 3: Abstract Test Suites (ATS)".

3GPP TS 34.229-5 [156]: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 5: Protocol conformance specification using 5G System (5GS)"

NOTE 1: The ATS is written in a standard testing language, TTCN-3, as defined in ETSI ES 201 873 Parts 1 to 3 [36] [37] [38].

NOTE 2: For conformance testing of the UTRAN requirements refer to 3GPP TS 34.123 Parts 1 to 3 [2] [3] [4].

NOTE 3: Further information on testing can be found in ETSI ETS 300 406[9] and ISO/IEC 9646-1 [7].

For at least a minimum set of services, the prose descriptions of test cases will have a matching detailed test case implemented in TTCN-3 (and provided in 3GPP TS 34.229-3 [6]).

1 Scope

The present document specifies the protocol conformance testing for the User Equipment (UE) supporting the Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

This is the first part of a multi-part test specification. The following information can be found in this part:

- the overall test structure;
- the test configurations;
- the conformance requirement and reference to the core specifications;
- the test purposes; and
- a brief description of the test procedure, the specific test requirements and short message exchange table.

The following information relevant to testing can be found in accompanying specifications:

- the applicability of each test case [5].

A detailed description of the expected sequence of messages can be found in the 3rd part of present test specification [6].

The Implementation Conformance Statement (ICS) pro-forma can be found in the 2nd part of the present test specification [5].

The present document is valid for UE implemented according to 3GPP Releases starting from Release 5 up to the Release indicated on the cover page of the present document.

Also, for clauses 8-18, 20 and 22, it is generally assumed that an IMS capable UE is compliant to GSMA PRD IR.92 [133] and GSMA PRD IR.94 [134]; any update of requirements in these GSMA PRD documents, which are relevant to the present document will be handled on a case by case basis, with due consideration given for grace period to be granted for the UE to comply to any updated requirements.

Editor's Note: it is to be clarified if we need to elaborate on clauses 19 and 21 here.

Test cases specified in Annexes G-K are targeted as indicated in their respective Scope sections.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document unless the context in which the reference is made suggests a different Release is relevant (information on the applicable release in a particular context can be found in e.g. test case title, description or applicability, message description or content).

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 34.123-1: "User Equipment (UE) conformance specification; Part 1: Protocol conformance specification".

[3] 3GPP TS 34.123-2: "User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".

[4] 3GPP TS 34.123-3: "User Equipment (UE) conformance specification; Part 3: Abstract Test Suites (ATS)".

[5] 3GPP TS 34.229-2: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".

[6] 3GPP TS 34.229-3: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 3: Abstract Test Suites (ATS)".

[7] ISO/IEC 9646-1: "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 1: General concepts".

[8] ISO/IEC 9646-7: "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[9] ETSI ETS 300 406: "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

[10] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[11] Void.

[12] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[13] Void.

[14] 3GPP TS 33.203: "Access security for IP based services".

[15] IETF RFC 3261: "SIP: Session Initiation Protocol".

[16] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[17] IETF RFC 3310: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[18] Void.

[19] IETF RFC 3608: "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[20] IETF RFC 3327: "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[21] IETF RFC 3329: "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[22] IETF RFC 3680: "A Session Initiation Protocol (SIP) Event Package for Registrations".

[23] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[24] IETF RFC 3320: “Signalling Compression (SigComp)”.

[25] IETF RFC 3485: “The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signalling Compression (SigComp)”.

[26] IETF RFC 3486: “Compressing the Session Initiation Protocol (SIP)”.

[27] IETF RFC 4566: "SDP: Session Description Protocol".

[28] Void.

[29] Void.

[30] IETF RFC 3264: "An Offer/Answer Model with the Session Description Protocol (SDP)".

[31] IETF RFC 3312: "Integration of Resource Management and Session Initiation Protocol (SIP)".

[32] 3GPP TS 23.003: "Numbering, addressing and identification".

[33] IETF RFC 3262: "Registration of provisional responses in Session Initiation Protocol (SIP)".

[34] Void.

[35] 3GPP TR 23.981 “Universal Mobile Telecommunications System (UMTS); Interworking aspects and migration scenarios for IPv4-based IP Multimedia Subsystem (IMS) implementations”.

[36] ETSI ES 201 873-1: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 1: TTCN-3 Core Language”.

[37] ETSI ES 201 873-2: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 2: TTCN-3 Tabular Presentation Format (TFT)".

[38] ETSI TR 201 873-3: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 3: TTCN-3 Graphical Presentation Format (GFT)".

[39] 3GPP TS 22.101: "Service aspects; Service principles".

[40] 3GPP TS 34.108: "Common test environments for User Equipment (UE); Conformance testing".

[41] Void.

[42] Void.

[43] Void.

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] IETF RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[49] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".

[50] IETF RFC 3263: "Session Initiation Protocol (SIP): Locating SIP Servers".

[51] IETF RFC 3319: "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[52] IETF RFC 1035: "Domain Names - Implementation And Specification".

[53] Void.

[54] Void.

[55] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[56] IETF RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".

[57] IETF RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[58] 3GPP TS 25.331: "Radio Resource Control (RRC) protocol specification".

[59] 3GPP TR 33.978: "Security aspects of early IP Multimedia Subsystem (IMS)".

[60] IETF RFC 3903: "Session Initiation Protocol (SIP) Extension for EventState Publication".

[61] IETF RFC 5627: "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)".

[62] IETF RFC 5628: "Reg Event Package Extension for GRUUs".

[63] IETF RFC 3840: "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

[64] IETF RFC 3841: "Caller Preferences for the Session Initiation Protocol (SIP)".

[65] 3GPP TS 24.173: "IMS Multimedia Telephony Communication Service and supplementary services; stage 3".

[66] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[67] IETF RFC 4867: "RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs".

[68] IETF RFC 6050: "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[69] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

[70] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[71] Void.

[72] IETF RFC 3515: "The Session Initiation Protocol (SIP) Refer Method".

[73] Void.

[74] Void.

[75] Void.

[76] Void.

[77] Void.

[78] Void.

[79] Void.

[80] Void.

[81] Void.

[82] Void.

[83] IETF RFC 7044: "An Extension to the Session Initiation Protocol (SIP) for Request History Information".

[84] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[85] Void".

[86] IETF RFC 4575: "A Session Initiation Protocol (SIP) Event Package for Conference State".

[87] 3GPP TS 24.247: "Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[88] IETF RFC 3842: "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)".

[89] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[90] 3GPP TS 24.341: "Support of SMS over IP networks; Stage 3".

[91] IETF RFC 3428: "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[92] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[93] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[94] 3GPP TS 36.508: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Common Test Environments for User Equipment (UE) Conformance Testing".

[95] 3GPP TS 24.615: "Communication Waiting (CW) using IP Multimedia (IM) Core Network (CN) subsystem".

[96] IETF RFC 3581: "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[97] IETF RFC 5031: "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

[98] IETF RFC 6442: "Location Conveyance for the Session Initiation Protocol".

[99] IETF RFC 4119: "A Presence-based GEOPRIV Location Object Format".

[100] Void.

[101] 3GPP TS 24.611: "Anonymous Communication Rejection (ACR) and Communication Barring (CB) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[102] 3GPP TS 24.607: "Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[103] 3GPP TS 24.608: "Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[104] 3GPP TS 24.629: "Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[105] 3GPP TS 24.623: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services ".

[106] 3GPP TS 24.604: "Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[107] 3GPP TS 24.606: "Message Waiting Indication (MWI) using IP Multimedia (IM) Core Network (CN) subsystem: Protocol specification".

[108] 3GPP TS 24.610: " Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[109] IETF RFC 5626: "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)".

[110] 3GPP TS 24.237: “IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) Service Continuity”.

[111] Void.

[112] 3GPP2 C.S0005-E: “Upper Layer (Layer 3) Signalling Standard for cdma2000 Spread Spectrum Systems”.

[113] 3GPP TS 31.121: "UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification".

[114] Void.

[115] Void.

[116] Void.

[117] 3GPP TS 34.109: "Terminal logical test interface; Special conformance testing functions".

[118] 3GPP TS 36.509: “Special conformance testing functions for User Equipment (UE)".

[119] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[120] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[121] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[122] IETF RFC 7254: "A Uniform Resource Name Namespace for the Global System for Mobile Communications Association (GSMA) and the International Mobile station Equipment Identity (IMEI)".

[123] 3GPP TS 27.007: " AT command set for User Equipment (UE)".

[124] IETF RFC 4835: "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

[125] IETF RFC 6809: "Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)".

[126] IETF RFC 4488: "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription".

[127] 3GPP TS 24.182: "IP Multimedia Subsystem (IMS) Customized Alerting Tones (CAT)".

[128] 3GPP TS 24.628: “Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem”.

[129] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[130] IETF RFC 6432: "Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses".

[131] IETF RFC 7462: "URNs for the Alert-Info Header Field of the Session Initiation Protocol (SIP)".

[132] IETF RFC 7315: "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP".

[133] GSMA PRD IR.92: "IMS Profile for Voice and SMS".

[134] GSMA PRD IR.94: "IMS Profile for Conversational Video Service".

[135] IETF RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[136] Void.

[137] IETF RFC 3311: "The Session Initiation Protocol (SIP) UPDATE Method".

[138] IETF RFC 5009: "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[139] IETF RFC 6086: “Session Initiation Protocol (SIP) INFO Method and Package Framework”.

[140] IETF RFC 6665: “SIP-Specific Event Notification”.

[141] 3GPP TS 23.167: " IP Multimedia Subsystem (IMS) emergency sessions".

[142] 3GPP TS 24.238: "Session Initiation Protocol (SIP) based user configuration; Stage3".

[143] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".[144] GSMA PRD NG.102: "IMS Profile for Converged IP Communications".

[145] GSMA PRD RCC.07: "Rich Communication Suite 7.0 – Advanced Communications Services and Client Specification".

[146] IETF RFC 4028 (April 2005): "Session Timers in the Session Initiation Protocol (SIP)".

[147] 3GPP TS 36.523-2: "User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS)proforma specification".

[148] GSMA PRD IR.51: “IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access”.

[149] IETF RFC 8147 (May 2017): "Next-Generation Pan-European eCall".

[150] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[151] GSMA PRD NG.108: "IMS Profile for Voice and SMS for UE category M1"

[152] 3GPP TS 24.390: " Unstructured Supplementary Service Data (USSD) using IP Multimedia (IM) Core Network (CN) subsystem IMS; Stage 3"

[153] IETF RFC 5646: " Tags for Identifying Languages"

[154] IETF RFC 7315: "P-Access-Network-Info ABNF Update"

[155] 3GPP TS 23.237: " IP Multimedia Subsystem (IMS) Service Continuity; Stage 2".

[156] 3GPP TS 34.229-5: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 5: Protocol conformance specification using 5G System (5GS)".

3 Definitions, symbols and abbreviations

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.1 Definitions

For the purposes of the present document, the following additional definitions apply:

Example: text used to clarify abstract rules by applying them literally

Floor: Floor(x) is the largest integer smaller than or equal to x.

Ceil: Ceil (x) is the smallest integer larger than or equal to x.

3.2 Symbols

For the purposes of the present document, the following additional symbols apply:

None.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAAA	Address (IP v6)
AKA	Authentication and Key Agreement
AKAv1-MD5	Authentication and Key Agreement version 1- Message-Digest 5
DUID	DHCP Unique Identifier
EF	Elementary File
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HMAC-MD5-96	Hashing for Message Authentication Code - Message-Digest 5 – 96 (bits)
HMAC-SHA-1-96	Hashing for Message Authentication Code - Secure Hash Algorithm 1 - 96 (bits)
ICS	Implementation Conformance Statement
IN	INternet
IPsec	IP Security
IXIT	Implementation eXtra Information for Testing
MIME	Multi purpose Internet Mail Extensions
MF	Master File
NAPTR	Naming Authority Pointer
P-CSCF	Proxy – Call Session Control Function
RTCP	Real Time Transport Control Protocol
SIGComp	SIGnalling Compression
SRV	SeRVice
SS	System Simulator

4 Overview

4.1 Test Methodology

4.1.1 Testing of optional functions and procedures

Any function or procedure which is optional, as indicated in the present document may be subject to a conformance test if it is implemented in the UE.

A declaration by the apparatus supplier (Implementation Conformance Statement (ICS)) is used to determine whether an optional function/procedure has been implemented (see ISO/IEC 9646-7 [8] for general information about ICS).

4.2 Implicit Testing

For some 3GPP signalling and protocol features conformance is not verified explicitly in the present document. This does not imply that correct functioning of these features is not essential, but that these are implicitly tested to a sufficient degree in other tests.

4.3 Conformance Requirements

The Conformance Requirements clauses in the present document are copy/paste from the relevant core specification where skipped text has been replaced with "...". References to clauses in the Conformance Requirements section of the test body refers to clauses in the referred specification, not sections in the present document.

5 Reference Conditions

The test cases are expected to be executed through the 3GPP radio interface. Details of the radio interfaces are outside the scope of this specification. The reference environments used by tests are specified in the test.

5.1 Generic setup procedures

A set of basic generic procedures for PDP Context Activation, P-CSCF Discovery and Registration are described in Annex C. These procedures are used in numerous test cases throughout the present document.

5.2 Transport protocols applied

For simplicity, UDP (*User Datagram Protocol*) is applied to the IMS test as default DL transport protocol.

NOTE: Which UL transport protocol is used in the test is decided by the UE.

6 PDP Context Activation

6.1 General Purpose PDP Context Establishment

Implicitly tested.

NOTE: This is implicitly tested as part of generic procedures.

6.2 General Purpose PDP Context Establishment (UE Requests for a Dedicated PDP Context)

6.2.1 Definition

Test to verify that the UE can establish a 'General Purpose PDP context' for SIP signalling.

6.2.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

NOTE 1: During the PDP context activation procedure, the UE and network negotiate whether the UE or the GPRS IP-CAN is responsible for the resource reservation applicable to all PDP contexts within the activated PDP address/APN pair, as described in 3GPP TS 24.008 [8].

When the bearer establishment is controlled by the UE, the UE shall choose one of the following options when performing establishment of this PDP context:

I. ….

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signalling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS information element.

NOTE 2: When the bearer establishment is controlled by the GPRS IP-CAN, the GGSN follows the procedures described in 3GPP TS 29.061 [11] in order to establish a dedicated PDP context for SIP signalling.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

Reference(s)

3GPP TS 24.229 [10], clause B.2.2.1.

6.2.3 Test purpose

To verify that the UE sends a correctly composed Activate PDP context request by setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

On receiving Activate PDP Context accept with IM CN Subsystem Signalling Flag not set within the Protocol Configuration Options IE, UE shall consider the PDP context as a General Purpose PDP context for SIP signalling.

6.2.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context for IMS

Test procedure

1) UE is configured for setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.

2) SS Responds with an Activate PDP Context Accept message by not setting IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE

3) P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.

4) UE sends an initial REGISTER request.

5) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA only), step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by not setting IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE
3				P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
4	→		REGISTER	UE sends initial registration for IMS services
5	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE 1: The default messages contents in annex A are used with condition "IMS security" or "GIBA".

Specific Message Contents:

Activate PDP Context Request (step 1)

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length	 (Note 2) 0002H (IM CN Subsystem Signalling Flag) 0 bytes

NOTE 2: UE may include additional containers also. If multiple containers are present they can be in any order.

Activate PDP Context Accept (step 2)

Case 1: UE supports IPv6 / IPv6 and IPv4

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents -- container 2 Identifier -- Container 2 Length -- Container 2 contents	 0001H (P-CSCF Address) (Included if ‘P-CSCF Server Address Request’ is received) 16 bytes IPV6 address of SS P-CSCF Server 0003H (DNS Address) (Included if ‘DNS Server Address Request’ is received) 16 bytes IPV6 address of SS DNS Server

Case 2: UE supports only IPv4

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents -- container 2 Identifier -- Container 2 Length -- Container 2 contents	 0001H (P-CSCF Address) 16 bytes IPV4 address of SS P-CSCF encoded as per 3GPP TR 23.981[35] 0003H (DNS Address) (Included if ‘DNS Server Address Request’ is received) 16 bytes IPV4 address of SS DNS server encoded as per 3GPP TR23.981[35]

REGISTER (Step 4)

Use the default message “REGISTER” in annex A.1.1 with condition A1 "Initial unprotected REGISTER"

6.2.5 Test requirements

1) In step 1, the UE shall set the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

2) In step 4, the UE shall send an initial REGISTER message using the established PDP context.

6.3 Dedicated PDP Context Establishment

6.3.1 Definition

Test to verify that the UE can establish a 'Dedicated PDP context' for SIP signalling.

6.3.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

NOTE 1: During the PDP context activation procedure, the UE and network negotiate whether the UE or the GPRS IP-CAN is responsible for the resource reservation applicable to all PDP contexts within the activated PDP address/APN pair, as described in 3GPP TS 24.008 [8].

When the bearer establishment is controlled by the UE, the UE shall choose one of the following options when performing establishment of this PDP context:

I. A dedicated PDP context for SIP signalling:

The UE shall indicate to the GGSN that this is a PDP context intended to carry IM CN subsystem-related signalling only by setting the IM CN Subsystem Signalling Flag. The UE may also use this PDP context for DNS and DHCP signalling according to the static packet filters as described in 3GPP TS 29.061 [11]. The UE can also set the Signalling Indication attribute within the QoS information element;

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signalling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS information element.

NOTE 2: When the bearer establishment is controlled by the GPRS IP-CAN, the GGSN follows the procedures described in 3GPP TS 29.061 [11] in order to establish a dedicated PDP context for SIP signalling.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

Reference(s)

3GPP TS 24.229 [10], clause B.2.2.1.

6.3.3 Test purpose

To verify that on receiving Activate PDP Context accept with IM CN Subsystem Signalling Flag included within the Protocol Configuration Options IE, UE shall consider the PDP context as a Dedicated PDP context for SIP signalling.

6.3.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context.

Test procedure

1) UE is configured for setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.

2) SS Responds with an Activate PDP Context Accept message by including IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE.

3) P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.

4) UE sends an initial REGISTER request.

5) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA only), step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by including IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE
3				P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
4	→		REGISTER	UE sends initial registration for IMS services
5	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE 1: The default messages contents in annex A are used with condition “IMS security“ or “GIBA”.

Specific Message Contents:

Activate PDP Context Request (step 1)

IE	Value/Remarks
Requested NSAPI	Any value
Protocol Configuration options	
- Additional Parameters	(Note 2)
-- container 1 Identifier	0002H (IM CN Subsystem Signalling Flag)
-- Container 1 Length	0 bytes

NOTE 2: UE may include additional containers also. If multiple containers are present they can be in any order.

Activate PDP Context Accept (step 2)

Case 1: UE supports IPv6 / IPv6 and IPv4

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- container 2 Identifier -- Container 2 Length -- Container 2 contents -- container 3 Identifier -- Container 3 Length -- Container 3 contents	 0002H (IM CN Subsystem Signalling Flag) 0 bytes 0001H (P-CSCF Address) (Included if 'P-CSCF Server Address Request' is received) 16 bytes IPV6 address of SS P-CSCF Server 0003H (DNS Address) (Included if 'DNS Server Address Request' is received) 16 bytes IPV6 address of SS DNS Server

Case 2: UE supports only IPv4

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- container 2 Identifier -- Container 2 Length -- Container 2 contents -- container 3 Identifier -- Container 3 Length -- Container 3 contents	 0002H (IM CN Subsystem Signalling Flag) 0 bytes 0001H (P-CSCF Address) 16 bytes IPV4 address of SS P-CSCF encoded as per 3GPP TR 23.981 0003H (DNS Address) (Included if 'DNS Server Address Request' is received) 16 bytes IPV4 address of SS DNS server encoded as per 3GPP TR 23.981[35]

REGISTER (Step 4)

Use the default message "REGISTER" in annex A.1.1 with condition A1 "Initial unprotected REGISTER" and with the following exceptions:

Header/param	Value/remark
Contact	
feature-param	Not checked

6.3.5 Test requirements

1) In step 1, the UE shall set the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

2) In step 4, the UE shall send an initial REGISTER message using the established PDP context.

7 P-CSCF Discovery

7.1 P-CSCF Discovery via PDP Context

7.1.1 Definition

Test to verify that the UE can establish a PDP context for SIP signalling and acquire P-CSCF address(es) during PDP Context Activation procedure.

7.1.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

NOTE 1: During the PDP context activation procedure, the UE and network negotiate whether the UE or the GPRS IP-CAN is responsible for the resource reservation applicable to all PDP contexts within the activated PDP address/APN pair, as described in 3GPP TS 24.008 [8].

When the bearer establishment is controlled by the UE, the UE shall choose one of the following options when performing establishment of this PDP context:

I. …

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signalling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS information element.

NOTE 2: When the bearer establishment is controlled by the GPRS IP-CAN, the GGSN follows the procedures described in 3GPP TS 29.061 [11] in order to establish a dedicated PDP context for SIP signalling.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

The UE can indicate a request for prioritised handling over the radio interface by setting the Signalling Indication attribute (see 3GPP TS 23.107 [4A]). The general QoS negotiation mechanism and the encoding of the Signalling Indication attribute within the QoS information element are described in 3GPP TS 24.008 [8].

NOTE 3: A general-purpose PDP Context can carry both IM CN subsystem signalling and media, in case the media does not need to be authorized by Policy and Charging control mechanisms as defined in 3GPP TS 29.212 [13C] and Service Based Local Policy mechanisms defined in 3GPP TS 29.207 [12] and the media stream is not mandated by the P-CSCF to be carried in a separate PDP Context.

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. …

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

From 3GPP TR 23.981 [35]:

The existing P-CSCF discovery mechanism are either IPv6 specific or use Release 5 or later GPRS. For an IPv4 based IMS implementation, operators may need other mechanisms not currently defined as possible options in 3GPP IMS.

The following mechanisms need to be evaluated for P-CSCF discovery in IPv4:

a) the address of the P-CSCF can be requested by the UE and returned by the GGSN at PDP context establishment time. An IPv4 UE would need to obtain an IPv4 address as part of this exchange.

If the PDP context established is of PDP type IPv4, then the GGSN may provide an IPv4 P-CSCF address. This does not preclude scenarios, where the GGSN returns an IPv6 P-CSCF address at IPv4 PDP context establishment, e.g. for the support of tunnelling (see clause 5.3.4.3), or both IPv4 and IPv6 P-CSCF addresses. If the PDP type is IPv4 then it is recommended that the GGSN always return both IP versions, if it is capable, using the existing capabilities to send multiple P-CSCF addresses within the PCO IE.

According to TS 24.008 [9], the P-CSCF address in the PCO field is an IPv6 address. Thus there are at least two possible approaches: The first approach would be to avoid any changes to or deviations from TS 24.008 [9] and use the existing methods to transfer an IPv4 address as an IPv6 address ("IPv6 address with embedded IPv4 address", as defined in RFC 2373 [10]). In such a case, the use of “IPv4 mapped addresses” as defined in RFC 2373 [10] is recommended.

The second approach would set the PCO field length to 4 and put the IP address in the content field. This would be a straightforward generalization of the specified method.

Reference(s)

3GPP TS 24.229 [10], clause B.2.2.1.

3GPP TR 23.981 [35], clause 5.2.1.

7.1.3 Test purpose

To verify that the UE sends a correctly composed Activate PDP context request message requesting for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE.

On receiving Activate PDP Context accept with IM CN Subsystem Signalling Flag not included within the Protocol Configuration Options IE and list of P-CSCF IPv6/IPv4 addresses included, UE shall consider the PDP context as a general purpose PDP context for SIP signalling and P-CSCF discovery procedure to be successful.

7.1.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context for IMS.

Test procedure

1) UE is configured for setting request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.

2) SS responds with an Activate PDP Context Accept including list of P-CSCF IPv6 and IPv4 addresses. IPv4 addresses are encoded as per 3GPP TR 23.981[35] clause 5.2.1.

3) UE sends an initial REGISTER request.

4) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA only), step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting request for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by including list of P-CSCF addresses
3	→		REGISTER	UE sends initial registration for IMS services
4	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 or step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE 1: The test sequence is identical for IPv4 and IPv6 except the message contents of Activate PDP Context Accept message. For a UE supporting both IPv4 and IPv6, only IPv6 option need to be executed.

NOTE 2: The default messages contents in annex A are used with condition “IMS security “ or “GIBA”.

Specific Message Contents:

Activate PDP Context Request (step 1)

NOTE 3: Containers can be in any order.

IE	Value/Remarks
Requested NSAPI Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- container 2 Identifier -- Container 2 Length	Any value 0001H (P-CSCF Address Request); 0 bytes 0003H (DNS Server Address Request) (Optional) 0 bytes

Activate PDP Context Accept (step 2)

Case 1: UE supports IPv6 / IPv6 and IPv4

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents -- container 2 Identifier -- Container 2 Length -- Container 2 contents	 0001H (P-CSCF Address) 16 bytes IPV6 address of SS P-CSCF Server 0003H (DNS Address) (Included if ‘DNS Server Address Request’ is received) 16 bytes IPV6 address of SS DNS Server

Case 2: UE supports "IPv6 address with embedded IPv4 address" in PCO IE

IE	Value/Remarks
- Additional Parameters	
Protocol Configuration options - Additional Parameters -- container 2 Identifier -- Container 2 Length -- Container 2 contents -- container 3 Identifier -- Container 3 Length -- Container 3 contents	 0001H (P-CSCF Address) 16 bytes IPV4 address of SS encoded as per 3GPP TR 23.981[35] option 1 0003H (DNS Address) (Included if 'DNS Server Address Request' is received) 16 bytes IPV4 address of SS DNS server encoded as per 3GPP TR 23.981[35] option 1

Case 3: UE supports IPv4 address in PCO IE

IE	Value/Remarks
- Additional Parameters	
Protocol Configuration options - Additional Parameters -- container 2 Identifier -- Container 2 Length -- Container 2 contents -- container 3 Identifier -- Container 3 Length -- Container 3 contents	 0001H (P-CSCF Address) 4 bytes IPV4 address of SS encoded as per 3GPP TR 23.981[35] option 2 0003H (DNS Address) (Included if 'DNS Server Address Request' is received) 4 bytes IPV4 address of SS DNS server encoded as per 3GPP TR 23.981[35] option 2

REGISTER (Step 3)

Use the default message "REGISTER" in annex A.1.1 with condition A1 "Initial unprotected REGISTER" and with the following exceptions:

Header/param	Value/remark
Contact	
feature-param	Not checked

7.1.5 Test requirements

1) In step 1, the UE shall request for P-CSCF address to the GGSN within the Protocol Configuration Options IE.

2) In step 3, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.2 P-CSCF Discovery via DHCP – IPv4

7.2.1 Definition

Test to verify that UE will perform P-CSCF discovery procedure via DHCP.

7.2.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. …

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network.

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

From 3GPP TR 23.981[35]:

The following mechanisms need to be evaluated for P-CSCF discovery in IPv4:

...

b) based on DHCP. Currently the specifications limit this to the IPv6 methods for DHCP. In order for this method to be used by an IPv4 UE, it needs to be identified how IPv4 DHCP is used to obtain the P-CSCF address. A solution that provides access independence would be that an IPv4 P-CSCF and IPv4 UE support configuration of the appropriate P-CSCF information via DHCPv4. In this solution, use of DHCP provides the UE with the fully qualified domain name of a P-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the P-CSCF name. When using DHCP/DNS procedure for P-CSCF discovery with IPv4 GPRS-access, the GGSN acts as DHCP Relay agent relaying DHCP messages between UE and the DHCP server. This is necessary to allow the UE to properly interoperate with the GGSN. This solution however requires that a UE supporting early IPv4 implementations would support DHCPv4.

Reference(s)

3GPP TS 24.229 [10], clause B.2.2.1.

3GPP TR 23.981 [35], clause 5.2.1.

7.2.3 Test purpose

To verify UE shall initiate and successfully complete a P-CSCF discovery procedure via DHCP when P-CSCF address is not provided as part of PDP Context Activation procedure.

7.2.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services. UE is not configured for using static P-CSCF address. UE has established a PDP context (No P-CSCF address information provided).). If UE sets flag ‘DNS Server Address Request' in PCO of PDP Context Request, DNS server address list is provided in PDP Context Accept message.

Test procedure

1) If UE already knows DHCP server address or is configured to send DHCPINFORM message to the limited (all 1s) broadcast address, it goes to step 3. Otherwise, UE sends DHCPDISCOVER message locating a server.
2) SS responds by DHCPOFFER message.
3) UE sends DHCPINFORM message requesting for P-CSCF address(es) in options field.
4) SS responds by DHCPACK message providing the domain names of P-CSCF address(es) and giving DNS server address.
5) UE initiates a DNS NAPTR query to select the transport protocol. UE’s configured to use specific Transport protocol on default ports, can skip steps 5 to 8 and go directly to step 9.
6) SS responds with NAPTR response.
7) UE initiates a DNS SRV query.
8) SS responds with SRV response.
9) UE initiates a DNS A query
10) SS responds with DNS A response.
11) UE sends an initial REGISTER request.
12) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA only), step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		DHCPDISCOVER	Optionally sent if UE does not have DHCP server address and is not configured to send DHCPINFORM message to the limited (all 1s) broadcast address.
2	←		DHCPOFFER	Sent if DHCP Discover message is received.
3	→		DHCPINFORM	Requesting P-CSCF Address(es)
4	←		DHCPACK	Including P-CSCF Address(es)
5	→		DNS NAPTR Query	UE configured to use specific Transport protocol on default ports, can skip steps 5 to 8 and go directly to step 9
6	←		DNS NAPTR Response	
7	→		DNS SRV Query	
8	←		DNS SRV Response	
9	→		DNS A Query	
10	←		DNS A Response	
11	→		REGISTER	UE sends initial registration for IMS services
12	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE 1: The default messages contents in annex A are used with condition “IMS security “ or “GIBA” when applicable

Specific Message Contents:

DHCPDISCOVER (step 1)

Use the default message in annex B

DHCPOFFER (step 2)

Use the default message in annex B

DHCPINFORM (step 3)

Use the default message in annex B with the following exceptions

Field	Value/Remarks
Options	(Note 2)
- code	53 (DHCP Message Type)
- len	1
-Type	2 (DHCP OFFER)
option-code - option-len	55 (Parameter Request List) Set to number of values requested for configuration parameters
Option code	120 (SIP Server Option) (Note 3)
Option code	6(Domain Server) Optionally present

NOTE 2: Other options may also be present

NOTE 3: Other option codes may also be present and options can be in any order

DHCPACK (step 4)

Use the default message in annex B.2 with the following exceptions

Field	Value/Remarks
option-code - option-len -enc	120 (SIP Server option) Length of encoded server domain address +1 (for enc field) 0
Domain-address 1	SS P-CSCF server domain AddressRFC 3361[57]
option-code - option-len	6 (DNS option RFC 2132[49]))(Included only if requested in DHCP INFORM) 4
DNS Address	4 byte IPv4 address of DNS server

DNS NAPTR Query (step 5)

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

DNS NAPTR Response (step 6)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

DNS SRV Query (step 7)

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

DNS SRV Response (step 8)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	NAPTR
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

DNS A Query (step 9)

Case 1: steps 5 to 8 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 8 based on priority and weight RFC 2782[56]
QCLASS=	IN
QTYPE=	A

Case 2: steps 5 to 8 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 4.
QCLASS=	IN
QTYPE=	A

DNS A Response (step 10)

IE	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	A
A or AAAA records	Includes resolved IP address(es).

7.2.5 Test requirements

1) In step 3, the UE shall initiate a P-CSCF discovery employing DHCP.

2) After step 4, the UE shall initiate a DNS query for domain address to IPv4 address translation.

3) In step 11, the UE shall send an initial REGISTER message using the discovered P-CSCF IPv4 address.

7.3 P-CSCF Discovery via DHCP – IPv4 (UE Requests P-CSCF discovery via PCO)

7.3.1 Definition

Test to verify that on not receiving P-CSCF Address(es) in PCO, UE will perform P-CSCF discovery procedure employing DHCP.

7.3.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

...

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network.

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

From 3GPP TR 23.981[35]:

The following mechanisms need to be evaluated for P-CSCF discovery in IPv4:

...

b) based on DHCP. Currently the specifications limit this to the IPv6 methods for DHCP. In order for this method to be used by an IPv4 UE, it needs to be identified how IPv4 DHCP is used to obtain the P-CSCF address. A solution that provides access independence would be that an IPv4 P-CSCF and IPv4 UE support configuration of the appropriate P-CSCF information via DHCPv4. In this solution, use of DHCP provides the UE with the fully qualified domain name of a P-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the P-CSCF name. When using DHCP/DNS procedure for P-CSCF discovery with IPv4 GPRS-access, the GGSN acts as DHCP Relay agent relaying DHCP messages between UE and the DHCP server. This is necessary to allow the UE to properly interoperate with the GGSN. This solution however requires that a UE supporting early IPv4 implementations would support DHCPv4.

Reference(s)

3GPP TS 24.229 [10], clause B.2.2.1.

3GPP TR 23.981 [35], clause 5.2.1.

7.3.3 Test purpose

To verify that the UE sends a correctly composed Activate PDP context request message requesting for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE.

On receiving Activate PDP Context accept not including P-CSCF address(es) in PCO, UE will initiate a P-CSCF discovery procedure employing DHCP/DNS.

7.3.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context. UE is not configured for using static P-CSCF address.

Test procedure

1) UE is configured for requesting P-CSCF address(es) in Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.
2) SS Responds with an Activate PDP Context Accept message by not including P-CSCF Address(es). If a UE already knows DHCP server address, it goes to step 5. If UE sets flag ‘DNS Server Address Request’ in PCO of PDP Context Request, DNS server address list is provided in PDP context Accept message.
3) If UE is configured to send DHCPINFORM message to the limited (all 1s) broadcast address, it goes to step 5. Otherwise, UE sends DHCPDISCOVER message locating a server.
4) SS responds by DHCPOFFER message.
5) UE sends DHCPINFORM message requesting for P-CSCF address(es) in options field.
6) SS responds by DHCPACK message providing the domain names of P-CSCF address(es) and giving a DNS server address.
7) UE initiates a DNS NAPTR query to select the transport protocol. UE’s configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11.
8) SS responds with NAPTR response.
9) UE initiates a DNS SRV query.
10) SS responds with SRV response.
11) UE initiates a DNS A or query.
12) SS responds with DNS A or response.
13) UE sends an initial REGISTER request.
14) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA only), step 5.

Expected sequence

Step	Direction UE	Direction SS	Message	Comment
1	→		Activate PDP Context Request	UE sends this PDU by setting request for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by not including P-CSCF address(es). If UE sets flag 'DNS Server Address Request' in PCO of PDP Context Request, DNS server address list is provided in PDP context Accept message. If UE knows DHCP server address, goes to step 5.
3	→		DHCPDISCOVER	Optionally sent if UE is not configured to send DHCPINFORM message to the limited (all 1s) broadcast address.
4	←		DHCPOFFER	Sent if DHCP Discover message is received.
5	→		DHCPINFORM	Requesting P-CSCF Address(es)
6	←		DHCPACK	Including P-CSCF Address(es)
7	→		DNS NAPTR Query	UE's configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11
8	←		DNS NAPTR Response	
9	→		DNS SRV Query	
10	←		DNS SRV Response	
11	→		DNS A or AAAA Query	
12	←		DNS A or AAAA Response	
13	→		REGISTER	UE sends initial registration for IMS services
14	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE 1: The default messages contents in annex A are used with condition "IMS security " or "GIBA" when applicable

Specific Message Contents:

Activate PDP Context Request (step 1)

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length	 0001H (P-CSCF Address Request) 0 bytes

Activate PDP Context Accept (step 2)

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents	Present only if 'DNS Server Address Request' received in Request message 0003H (DNS Address) 16 bytes IPV4 address of SS DNS server encoded as per 3GPP TR 23.981[35]

DHCPDISCOVER (step 3)

Use the default message in annex B.

DHCPOFFER (step 4)

Use the default message in annex B.

DHCPINFORM (step 5)

Use the default message in annex B with the following exceptions:

Field	Value/Remarks
Options - code - len -Type	(Note 2) 53 (DHCP Message Type) 1 2 (DHCP OFFER)
option-code - option-len	55 (Parameter Request List) Set to number of values requested for configuration parameters
Option code	120 (SIP Server Option) (Note 3)
Option code	6(Domain Server) Optionally present

NOTE 2: Other options may also be present.

NOTE 3: Other option codes may also be present and options can be in any order.

DHCPACK (step 6)

Use the default message in annex B with the following exceptions:

Field	Value/Remarks
option-code - option-len -enc	120 (SIP Server option) Length of encoded server domain address +1 (for enc field) 0
Domain-address 1	SS P-CSCF server domain AddressRFC 3361[57]
option-code - option-len	6 (DNS option RFC 2132[49]) (Included only if requested in DHCP INFORM) 4
DNS Address	4 byte IPv4 address of DNS server

DNS NAPTR Query (step 7)

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

DNS NAPTR Response (step 8)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

DNS SRV Query (step 9)

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

DNS SRV Response (step 10)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	NAPTR
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

DNS A Query (step 11)

Case 1: steps 7 to 10 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 8 based on priority and weight RFC 2782[56]
QCLASS=	IN
QTYPE=	A

Case 2: steps 7 to 10 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 6.
QCLASS=	IN
QTYPE=	A

DNS A Response (step 12)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	A
A records	Includes resolved IP address(es).

7.3.5 Test requirements

1) In step 1, the UE shall set the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

2) After step 2, the UE shall initiate a P-CSCF discovery employing DHCP.

3) In step 3, if the UE has no knowledge of a DHCP server address and is not configured to send a DHCPINFORM message to the limited (all 1s) broadcast address then it shall send a DHCPDISCOVER message.

4) In step 5, the UE shall send a DHCPRequest message, including options filed with option code 120.

5) After step 6, the UE shall initiate a DNS query.

6) In step 13, the UE shall send an initial REGISTER message using the discovered P-CSCF IPv4 address.

7.4 P-CSCF Discovery by DHCP - IPv6

7.4.1 Definition

Test to verify that UE will perform P-CSCF discovery procedure employing DHCP.

7.4.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. …

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network.

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv4 or IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

.

Reference(s)

3GPP TS 24.229 [10], clause B.2.2.1,.

7.4.3 Test purpose

To verify UE shall initiate and successfully complete a P-CSCF discovery procedure via DHCP when P-CSCF address is not provided as part of PDP Context Activation procedure.

7.4.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services. UE has established a PDP context. UE has not received P-CSCF address(es) during PDP context establishment. If UE sets flag 'DNS Server Address Request' in PCO of PDP Context Request, DNS server address list is provided in PDP Context Accept message.

Test procedure

1. UE may send DHCP SOLICIT message locating a server. If UE is configured to send Information-Request to 'All_DHCP_Relay_Agents_and_Servers' multicast address, test case starts at step 3.
2. SS responds with DHCP ADVERTISE message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 11, else go to step 5
3. UE sends DHCP Query requesting either IP address(es) of P-CSCF server(s) or domain names of P-CSCF server(s) and DNS Server.
4. SS responds by DHCP Reply message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 11.
5. UE initiates a DNS NAPTR query to select the transport protocol. UE's configured to use specific Transport protocol on default ports, can skip steps 5 to 8 and go directly to step 9.
6. SS responds with NAPTR response.
7. UE initiates a DNS SRV query.
8. SS responds with SRV response.
9. UE initiates a DNS AAAA query.
10. SS responds with DNS AAAA response.
11. UE sends an initial REGISTER request.
12. Continue test execution with the Generic test procedure, Annex C.2, step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		DHCP SOLICIT	Optional message
2	←		DHCP ADVERTISE	Sent if DHCP Solicit message is received. Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 11, else go to step 5
3	→		DHCP Information-Request	Requesting P-CSCF Address(es) (Note 1)
4	←		DHCP Reply	Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 11.
5	→		DNS NAPTR Query	UE's configured to use specific Transport protocol on default ports, can skip steps 5 to 8 and go directly to step 9
6	←		DNS NAPTR Response	
7	→		DNS SRV Query	
8	←		DNS SRV Response	
9	→		DNS AAAA Query	
10	←		DNS AAAA Response	
11	→		REGISTER	UE sends initial registration for IMS services
12	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE 1: UE may request all options in one Information Request or send multiple Information Requests. If UE opts for multiple Information Request transmissions, SS transmits accordingly multiple Reply messages including corresponding requested options.

NOTE 2: The default messages contents in annex A are used with condition "IMS security" or "GIBA".

Specific Message Contents:

Step 1: DHCP SOLICIT*

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code	OPTION_ORO (6)
- option-len	2 times number of requested options
-requested-option-code-1	OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22)
- requested-option-code-2	OPTION_DNS_SERVERS (23)
- requested-option-code-3	OPTION_DOMAIN_LIST (24)

NOTE 3: Options can be optionally present and option codes can be in any order

NOTE 4: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 2: DHCP ADVERTISE

Use the default message in annex B.1 with the following exceptions

NOTE 5: Options are included only if corresponding Requests are received.

Case 1: (OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 1

Options	Value/Remarks
option-code - option-len	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51]
Domain-address 1	SS P-CSCF server domain address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

NOTE 6: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 1

Options	Value/Remarks
option-code - option-len	OPTION_SIP_SERVER_A (22) 128
Domain-address 1	IPv6 address of SS P-CSCF Server
option-code - option-len	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

NOTE 7: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 3: DHCP Information-Request

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code - option-len - requested-option-code-1 - requested-option-code-2 - requested-option-code-3	OPTION_ORO (6) 2 * number of requested options OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22) OPTION_DNS_SERVERS (23)(Optional) OPTION_DOMAIN_LIST (24) (Optional)

NOTE 8: All options can be either received in one message or multiple messages. If more than one option codes present they can be in any order.

NOTE 9: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 4: DHCP Reply

Use the default message in annex B.1 with the following exceptions

NOTE 10: Options are included only if corresponding Requests are received.

Case 1: OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 3

Options	Value/Remarks
option-code - option-len	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51]
Domain-address 1	SS P-CSCF server domain Address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

NOTE 11: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 3

Options	Value/Remarks
option-code - option-len	OPTION_SIP_SERVER_A (22) 128
Domain-address 1	IPv6 address of SS P-CSCF Server
option-code - option-len	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035 [52]

NOTE 12: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 5: DNS NAPTR Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

Step 6: DNS NAPTR Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

Step 7: DNS SRV Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

Step 8: DNS SRV Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	SRV
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

Step 9: DNS AAAA Query

Case 1: steps 5 to 8 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 8 based on priority and weight RFC 2782[56]
QCLASS=	IN
QTYPE=	AAAA

Case 2: steps 5 to 8 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 2 or 4.
QCLASS=	IN
QTYPE=	AAAA

Step 10: DNS AAAA Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in AAAA Query
QCLASS=	IN
QTYPE=	AAAA
AAAA records	Includes resolved IP address(es).

7.4.5 Test requirements

1. In step 1, the UE shall initiate a P-CSCF discovery employing DHCP.
2. After steps 2 and 4, if a P-CSCF IPv6 address is received then the UE will consider the P-CSCF discovery procedure successful, else the UE will initiate a DNS query for domain address to IPv6 address translation.
3. In step 11, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.5 P-CSCF Discovery by DHCP-IPv6 (UE Requests P-CSCF discovery by PCO)

7.5.1 Definition

Test to verify that on not receiving P-CSCF Address(es) in PCO, will perform P-CSCF discovery procedure employing DHCP.

7.5.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8]re;

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

...

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or
- the UE is roaming and the P-CSCF is to be discovered in the visited network.

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv4 or IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

Reference(s)

3GPP TS 24.229 [10], clause B.2.2.1,.

7.5.3 Test purpose

To verify that the UE sends a correctly composed Activate PDP context requesting for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE.

On receiving Activate PDP Context accept not including P-CSCF address(es) in PCO IE, will initiate a P-CSCF discovery procedure employing DHCP.

7.5.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context.

Test procedure

1. UE is configured for requesting P-CSCF address(es) in Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.
2. SS Responds with an Activate PDP Context Accept message by not including P-CSCF address(es). If UE sets flag ‘DNS Server Address Request’ in PCO of PDP Context Request, DNS server address list is provided in PDP Context Accept message.
3. UE may send DHCP Solicit message locating a server. If UE is configured to send Information-Request to ‘All_DHCP_Relay_Agents_and_Servers’ multicast address, go to step 5.
4. SS responds by Advertise message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 13 else go to step 7.
5. UE sends DHCP Information-Request Query requesting either IP address(es) of P-CSCF server(s) or domain names of P-CSCF server(s) and DNS Server.
6. SS responds by DHCP Reply message.. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 13.
7. UE initiates a DNS NAPTR query to select the transport protocol. UE’s configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11.
8. SS responds with NAPTR response.
9. UE initiates a DNS SRV query.
10. SS responds with SRV response.
11. UE initiates a DNS AAAA query.
12. SS responds with DNS AAAA response.
13. UE sends an initial REGISTER request.
14. Continue test execution with the Generic test procedure, Annex C.2, step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting request for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by not including P-CSCF address(es). If UE sets flag 'DNS Server Address Request' in PCO of PDP Context Request, DNS server address list is provided.
3	→		DHCP SOLICIT	Optional message
4	→		DHCP ADVERTISE	Sent if DHCP Solicit message is received. Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 13 else go to step 7
5	→		DHCP Information-Request	Requesting P-CSCF Address(es) (Note 1)
6	←		DHCP Reply	Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 13.
7	→		DNS NAPTR Query	UE's configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11
8	←		DNS NAPTR Response	
9	→		DNS SRV Query	
10	←		DNS SRV Response	
11	→		DNS AAAA Query	
12	←		DNS AAAA Response	
13	→		REGISTER	UE sends initial registration for IMS services
14	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE 1: UE may request all options in one Information Request or send multiple Information Requests. If UE opts for multiple Information Request transmissions, SS transmits accordingly multiple Reply messages including corresponding requested options.

NOTE 2: The default messages contents in annex A are used with condition "IMS security" or "GIBA".

Specific Message Contents:

Step 1: Activate PDP Context Request

Options	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- container 2 Identifier -- Container 2 Length	 0001H (P-CSCF Address Request) 0 bytes 0003H (DNS Server Address Request) (Optionally present) 0 bytes

Step 2: Activate PDP Context Accept

Options	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents	(Included if 'DNS Server Address Request' is received) 0003H (DNS Address) 16 bytes IPV6 address of SS DNS Server

Step 3: DHCP SOLICIT*

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code - option-len - requested-option-code-1 - requested-option-code-2 - requested-option-code-3	OPTION_ORO (6) 2 times number of requested options OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22) OPTION_DNS_SERVERS (23) OPTION_DOMAIN_LIST (24)

NOTE 3: Options can be optionally present and option codes can be in any order

NOTE 4: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 4: DHCP ADVERTISE

Use the default message in annex B.1 with the following exceptions

NOTE 5: Options are included only if corresponding Requests are received.

Case 1: OPTION_SIP_SERVER_D (21) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 3

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51] SS P-CSCF server domain Address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

NOTE 6: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 3

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_A (22) 128 IPv6 address of SS P-CSCF Server
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len searchlist	OPTION_DOMAIN_LIST (24) Length of Domain search list List of Domain Names encoded as per RFC 1035 [52]

NOTE 7: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 5: DHCP Information-Request

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code - option-len -requested-option-code-1 - requested-option-code-2 - requested-option-code-3	OPTION_ORO (6) 2 (Note 8) number of requested options OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22) OPTION_DNS_SERVERS (23)(Optional) OPTION_DOMAIN_LIST (24) (Optional)

NOTE 8: All options can be either received in one message or multiple messages. If more than one option codes present they can be in any order.

NOTE 9: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 6: DHCP Reply

Use the default message in annex B.1 with the following exceptions

NOTE 10: Options are included only if corresponding Requests are received.

Case 1: (OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 5

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51] SS P-CSCF server domain Address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len searchlist	OPTION_DOMAIN_LIST (24) Length of Domain search list List of Domain Names encoded as per RFC 1035[52]

NOTE 11: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 5

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_A (22) 128 IPv6 address of SS P-CSCF Server
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len searchlist	OPTION_DOMAIN_LIST (24) Length of Domain search list List of Domain Names encoded as per RFC 1035 [52]

NOTE 12: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 7: DNS NAPTR Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

Step 8: DNS NAPTR Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

Step 9: DNS SRV Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

Step 10: DNS SRV Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	SRV
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

Step 11: DNS AAAA Query

Case 1: steps 7 to 10 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 10 based on priority and weight RFC 2782[56]
QCLASS=	IN
QTYPE=	AAAA

Case 2: steps 7 to 10 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 4 or 6.
QCLASS=	IN
QTYPE=	AAAA

Step 12: DNS AAAA Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in AAAA Query
QCLASS=	IN
QTYPE=	AAAA
AAAA records	Includes resolved IP address(es).

7.5.5 Test requirements

1. In step 1, the UE shall set the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.
2. After step 2, the UE shall initiate a P-CSCF discovery employing DHCP.
3. After step 6, if a P-CSCF IPv6 address is received then the UE will consider the P-CSCF discovery procedure successful, else the UE will initiate a DNS query for domain address to IPv6 address translation.
4. In step 13, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.6 P-CSCF Discovery by DHCP – IPv6 (UE does not Request P-CSCF discovery by PCO, SS includes P-CSCF Address(es) in PCO)

7.6.1 Definition

Test to verify that on not receiving P-CSCF Address(es) in PCO, will perform P-CSCF discovery procedure employing DHCP.

7.6.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

...

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network.

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv4 or IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

Reference(s)

3GPP TS 24.229 [10], clause B.2.2.1

7.6.3 Test purpose

To verify that a UE, which has not requested for P-CSCF address in PDP context activate message, receives P-CSCF address, may accept the P-CSCF address or ignore it and hence initiate P-CSCF discovery by DHCP.

7.6.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context.

Test procedure

1. UE is configured for not requesting P-CSCF addresses in PCO.
2. SS Responds with an Activate PDP Context Accept message by including P-CSCF Address(es). UE can either assume P-CSCF procedure to be complete or neglect the P-CSCF address(es) in PDP context Accept. Test Ends if UE assumes P-CSCF procedure to be complete.
3. UE may send Solicit message locating a server. If UE is configured to send Information-Request to 'All_DHCP_Relay_Agents_and_Servers' multicast address, go to step 5.

4. SS responds by Advertise message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 13, else go to step 7.

5. UE sends DHCP Information-Request Query requesting either IP address(es) of P-CSCF server(s) or domain names of P-CSCF server(s) and DNS Server.

6. SS responds by DHCP Reply message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 13.

7. UE initiates a DNS NAPTR query to select the transport protocol. UE's configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11.

8. SS responds with NAPTR response.

9. UE initiates a DNS SRV query.

10. SS responds with SRV response.

11. UE initiates a DNS AAAA query.

12. SS responds with DNS AAAA response.

13. UE sends an initial REGISTER request.

14. Continue test execution with the Generic test procedure, Annex C.2, step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU not requesting for P-CSCF address(es)
2	←		Activate PDP Context Accept	SS Sends this response including P-CSCF Address(es). UE shall either ignore the received address, or use the address. If UE uses address, go to step 13.
3	→		DHCP SOLICIT	Optional message
4	←		DHCP ADVERTISE	Sent if DHCP Solicit message is received. Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 13, else go to step 7
5	→		DHCP Information-Request	Requesting P-CSCF Address(es) (Note 1)
6	←		DHCP Reply	Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 13.
7	→		DNS NAPTR Query	UE's configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11
8	←		DNS NAPTR Response	
9	→		DNS SRV Query	
10	←		DNS SRV Response	
11	→		DNS AAAA Query	
12	←		DNS AAAA Response	
13	→		REGISTER	UE sends initial registration for IMS services
14	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE 1: UE may request all options in one Information Request or send multiple Information Requests. If UE opts for multiple Information Request transmissions, SS transmits accordingly multiple Reply messages including corresponding requested options.

NOTE 2: The default messages contents in annex A are used with condition “IMS security “ or “GIBA” when applicable

Specific Message Contents:

Step 2: Activate PDP Context Accept

Options	Value/Remarks
Protocol Configuration options	
- Additional Parameters	
-- container 1 Identifier	0001H (P-CSCF Address)
-- Container 1 Length	16 bytes
-- Container 1 contents	IPV6 address of SS
-- container 2 Identifier	0003H (DNS Address)
-- Container 2 Length	16 bytes
-- Container 2 contents	IPV6 address of SS DNS Server

Step 3: DHCP SOLICIT (Note 3)

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code	OPTION_ORO (6)
- option-len	2 times number of requested options
-requested-option-code-1	OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22)
- requested-option-code-2	OPTION_DNS_SERVERS (23)
- requested-option-code-3	OPTION_DOMAIN_LIST (24)

NOTE 3: Options can be optionally present and option codes can be in any order

NOTE 4: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 4: DHCP ADVERTISE

Use the default message in annex B.1 with the following exceptions

NOTE 5: Options are included only if corresponding Requests are received.

Case 1: (OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 3

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51] SS P-CSCF server domain Address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len searchlist	OPTION_DOMAIN_LIST (24) Length of Domain search list List of Domain Names encoded as per RFC 1035 [52]

NOTE 6: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 3

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_A (22) 128 IPv6 address of SS P-CSCF Server
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len searchlist	OPTION_DOMAIN_LIST (24) Length of Domain search list List of Domain Names encoded as per RFC 1035 [52]

NOTE 7: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 5: DHCP Information-Request

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code	OPTION_ORO (6)
- option-len	2 (Note 8) number of requested options
-requested-option-code-1	OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22)
- requested-option-code-2	OPTION_DNS_SERVERS (23)(Optional)
- requested-option-code-3	OPTION_DOMAIN_LIST (24) (Optional)

NOTE 8: All options can be either received in one message or multiple messages. If more than one option codes present they can be in any order.

NOTE 9: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 6: DHCP Reply

Use the default message in annex B.1 with the following exceptions

NOTE 10: Options are included only if corresponding Requests are received.

Case 1: (OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 5

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51] SS P-CSCF server domain Address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len searchlist	OPTION_DOMAIN_LIST (24) Length of Domain search list List of Domain Names encoded as per RFC 1035 [52]

NOTE 11: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 5

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_A (22) 128 IPv6 address of SS P-CSCF Server
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len searchlist	OPTION_DOMAIN_LIST (24) Length of Domain search list List of Domain Names encoded as per RFC 1035 [52]

NOTE 12: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 7: DNS NAPTR Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

Step 8: DNS NAPTR Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

Step 9: DNS SRV Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

Step 10: DNS SRV Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	SRV
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

Step 11: DNS AAAA Query

Case 1: steps 7 to 10 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 10 based on priority and weight RFC 2782[56]
QCLASS=	IN
QTYPE=	AAAA

Case 2: steps 7 to 10 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 4 or 6.
QCLASS=	IN
QTYPE=	AAAA

Step 12: DNS AAAA Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in AAAA Query
QCLASS=	IN
QTYPE=	AAAA
AAAA records	Includes resolved IP address(es).

7.6.5 Test requirements

1. In step 1, the UE shall send a PDP Context Request message.
2. After step 2, the UE shall either ignore the received address, or use the address received.
3. If the UE ignores the P-CSCF address in step 2, then the UE will send a DHCP query in step 3.
4. After steps 4 and 6, if a P-CSCF IPv6 address is received then the UE will consider the P-CSCF discovery procedure successful, else the UE will initiate a DNS query for domain address to IPv6 address translation.
5. In step 13, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.7 Void

7.8 Void

7.9 Void

8 Registration

TCP (***Transmission Control Protocol***) is applied as DL transport protocol to the present clause.

8.1 Initial registration

8.1.1 Definition

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing the registration event package for the registered default public user identity.

8.1.2 Conformance requirement

[TS 24.229, clause C.2]:

In case the UE is loaded with a UICC that contains a USIM but does not contain an ISIM, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003. Also in this case, the UE shall derive new values every time the UICC is changed, and shall discard existing values if the UICC is removed.

NOTE: If there is an ISIM and a USIM on a UICC, the ISIM is used for authentication to the IM CN subsystem, as described in 3GPP TS 33.203. See also subclause 5.1.1.1A.

[TS 24.229, clause 5.1.1.1A]:

This subclause applies when a UE contains either an ISIM or a USIM.

The ISIM shall always be used for authentication to the IM CN subsystem, if it is present, as described in 3GPP TS 33.203.

The ISIM is preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one or more public user identities; and
- the home network domain name used to address the SIP REGISTER request

The first public user identity in the list stored in the ISIM is used in emergency registration requests.

In case the UE does not contain an ISIM, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to;

in accordance with the procedures in clause C.2.

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, mobile-initiated deregistration.

The UE shall not reveal to the user the temporary public user identity if the temporary public user identity is barred. The temporary public user identity is not barred if received by the UE in the P-Associated-URI header.

If the UE is unable to derive the parameters in this subclause for any reason, then the UE shall not proceed with the request associated with the use of these parameters and will not be able to register to the IM CN subsystem.

[TS 24.229, clause 5.1.1.2.1]:

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

When registering any public user identity belonging to the UE, the UE shall either use an already active pair of security associations or a TLS session to protect the REGISTER requests, or register the public user identity via a new initial registration procedure.

When binding any one of its public user identities to an additional contact address via a new initial registration procedure, the UE shall follow the procedures described in RFC 5626. The set of security associations or a TLS session resulting from this initial registration procedure will have no impact on the existing set of security associations or TLS sessions that have been established as a result of previous initial registration procedures. However, if the UE registers any one of its public user identities with a new contact address via a new initial registration procedure and does not employ the procedures described in RFC 5626, then the new set of security associations or TLS session shall replace any existing set of security association or TLS session.

If the UE detects that the existing security associations or TLS sessions associated with a given contact address are no longer active (e.g., after receiving no response to several protected messages), the UE shall:

- consider all previously registered public user identities bound to this security associations or TLS session that are only associated with this contact address as deregistered; and

- stop processing all associated ongoing dialogs and transactions that were using the security associations or TLS session associated with this contact address, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs).

The UE shall send the unprotected REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, or if the UE was pre-configured with the P-CSCF's IP address or domain name and was unable to obtain specific port information, the UE shall send the unprotected REGISTER request to the SIP default port values as specified in RFC 3261.

NOTE 1: The UE will only send further registration and subsequent SIP messages towards the same port of the P-CSCF for security mechanisms that do not require using negotiated ports for exchanging protected messages.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

[TS 24.229 Rel-8, clause 5.1.1.2.1]:

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4).

[TS 24.229 Rel-9, clause 5.1.1.2.1]:

…

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 4: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

[TS 24.229 Rel-8, clause 5.1.1.2.1]:

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header field value and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 4: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;

d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 5: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 6: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626, and the S-CSCF has followed the registration procedure as described in RFC 5627 or RFC 3261, i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626, the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626; or

NOTE 7: Upon replaces the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about the deregistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626; and

g) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223.[TS 24.229 Rel-9, clause 5.1.1.2.1]:

…

g) store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session; and

NOTE 9: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223.

[TS 24.229 Rel-10, clause 5.1.1.2.1]:

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE:

1) supports GRUU (see table A.4, item A.4/53);

2) supports multiple registrations;

3) has an IMEI available; or

4) has an MEID available;

the UE shall include a "+sip.instance" header field parameter containing the instance ID. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223 [143];

NOTE 3: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 4: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

1) if GRUU is supported, the option-tag "gruu"; and

2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header field value and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 6: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;

d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 7: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 8: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626, and the S-CSCF has followed the registration procedure as described in RFC 5627 or RFC 3261, i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626, the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626; or

NOTE 9: Upon replaces the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about the deregistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626;

g) store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session; and

NOTE 10: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223.

[TS 24.229, clause 5.1.1.2.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter, set to the value of the private user identity;
- the "realm" header field parameter, set to the domain name of the home network;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to an empty value; and
- the "response" header field parameter, set to an empty value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the port values see 3GPP TS 33.203.

b) additionally for the Contact header field, if the REGISTER request is protected by a security association, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field; and

d) a Security-Client header field set to specify the signalling plane security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203. The syntax of the parameters needed for the security association setup is specified in annex H of 3GPP TS 33.203. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329. The UE shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203, and shall announce support for them according to the procedures defined in RFC 3329.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, the UE shall additionally:

1) If the UE supports multiple registrations and the REGISTER request contained the "+sip.instance" header field parameter and the "reg-id" header field parameter in the Contact header field, and the "outbound" option-tag in the Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field. If the option-tag "outbound" is present, then the UE shall use the bidirectional flow as defined in RFC 5626 as follows:

   a) for UDP, the bidirectional flow consists of two unidirectional flows, i.e. the first unidirectional flow is identified with the UE's protected client port, the P-CSCF's protected server port, and the respective IP addresses. The UE uses this flow to send the requests and responses to the P-CSCF. The second unidirectional flow is identified with the P-CSCF's protected client port, the UE's protected server port and the IP addresses. The second unidirectional flow is used by the UE to receive the requests and responses from the P-CSCF; or

   b) for TCP, the bidirectional flow is the TCP connection between the UE and the P-CSCF. This TCP connection was established by the UE, i.e. from the UE's protected client port and the UE's IP address to the P-CSCF's protected server port and the P-CSCF's IP address. This TCP connection is used to exchange SIP messages between the UE and the P-CSCF; and

2) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

NOTE 3: If the UE receives Authentication-Info, it will proceed as described in RFC 3310.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229, clause 5.1.1.5.1]:

Authentication is performed during initial registration. A UE can be re-authenticated during subsequent reregistrations, deregistrations or registrations of additional public user identities. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

[TS 24.229 Rel-8, clause 5.1.1.5.1]:

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203;

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

3) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

   - the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

   - the "username" header field parameter, set to the value of the private user identity;

   - the "response" header field parameter that contains the RES parameter, as described in RFC 3310;

   - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

   - the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and

   - the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

   The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

[TS 24.229 Rel-9, clause 5.1.1.5.1]:

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field and labelled with the "mediasec" header field parameter specified in subclause 7.2A.7, if any; and

NOTE 1: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

   - the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

   - the "username" header field parameter, set to the value of the private user identity;

   - the "response" header field parameter that contains the RES parameter, as described in RFC 3310 [49];

   - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

   - the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and

   - the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

[TS 24.229, clause 5.1.1.5.1]:

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

NOTE 2: If the UE has registered multiple contact addresses, the UE can either send requests towards the P-CSCF over the newly established set of security associations, or use different UE's contact address and associated set of security associations when sending the requests towards the P-CSCF. Responses towards the P-CSCF that are sent via UDP will be sent over the same set of security associations that the related request was received on. Responses towards the P-CSCF that are sent via TCP will be sent over the same set of security associations that the related request was received on.

When the first request or response protected with the newly established set of security associations is received from the P-CSCF or when the lifetime of the old set of security associations expires, the UE shall delete the old set of security associations and related keys it may have with the P-CSCF after all SIP transactions that use the old set of security associations are completed.

[TS 24.229, clause 5.1.1.3]:

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680.

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

[TS 24.229 Rel-8, clause 5.1.1.3]:

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

g) a Contact header field set to contain:.

the same IP address or FQDN, and if multiple registrations is supported, its instance ID ("+sip.instance" header field parameter) and an "ob" SIP URI parameter as described in RFC 5626;

- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; and

- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial REGISTER request.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header field of the received response.

[TS 24.229 Rel-9, clause 5.1.1.3]:

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) void; and

g) void.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header field of the received response.

[TS 24.229, clause 5.1.2.1]:

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID header field, and the values of tags in To and From header fields).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package the UE shall perform the following actions:

- if a state attribute "active", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;

- if a state attribute "active" is received, and the UE supports GRUU (see table A.4, item A.4/53), then for each public user identity indicated in the notification that contains a <pub-gruu> element or a <temp-gruu> element or both (as defined in RFC 5628) then the UE shall store the value of those elements in association with the public user identity;

- if a state attribute "terminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered and shall remove any associated GRUUs.

NOTE 1: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity or when S-CSCF receives a Push-Profile-Request (PPR) from the HSS (as described in 3GPP TS 29.228) changing the status of a public user identity associated with a registered implicit set from barred to non-barred. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE. The implicitly registered public user identities may also belong to different service profiles. The here-described procedures provide a different mechanism (to the 200 (OK) response to the REGISTER request) to inform the UE about these automatically registered public user identities.

NOTE 2: RFC 5628 provides guidance on the management of temporary GRUUs, utilizing information provided in the reg event notification.

[TS 24.229, clause 5.1.2A.1.1]:

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using either a given contact address, or to the registration flow and the associated contact address the UE shall:

- if IMS AKA is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

- if SIP digest without TLS is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the port value of an unprotected port and the contact address where the UE expects to receive subsequent mid-dialog requests; and

  b) populate the Via header field of the request with the port value of an unprotected port and the respective contact address where the UE expects to receive responses to the request;

...

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

NOTE 13: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs and standalone transactions. The UE shall build a list of Route header field values made out of the following, in this order:

a) the P-CSCF URI containing the IP address or the FQDN learnt through the P-CSCF discovery procedures; and

b) the P-CSCF port based on the security mechanism in use:

- if IMS AKA or SIP digest with TLS is in use as a security mechanism, the protected server port learnt during the registration procedure;

- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is in use as a security mechanism, the unprotected server port used during the registration procedure;

c) and the values received in the Service-Route header field saved from the 200 (OK) response to the last registration or re-registration of the public user identity with associated contact address.

[TS 24.341, clause 5.3.2.2]

On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.1.1A, 5.1.1.2.1 5.1.1.2, 5.1.1.35.1.1.5.1, 5.1.2.1, 5.1.2A.1, C.2 and TS 24.341, clause 5.3.2.2.

8.1.3 Test purpose

1) To verify that UE correctly derives a private user identity, a temporary public user identity and a home network domain name from the IMSI parameter in the USIM if no ISIM is available on the UICC, according to the procedures described in 3GPP TS 23.003 [32] clause 13 or alternatively uses the values retrieved from ISIM, if ISIM is present; and

2) To verify that the UE sends a correctly composed initial REGISTER request to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.1.2; and TS 24.341 [90] clause 5.3.2.2 (if UE supports SM-over-IP receiver marked as yes)

3) To verify that after receiving a valid 401 (Unauthorized) response from S-CSCF for the initial REGISTER sent, the UE correctly authenticates itself by sending another REGISTER request with correctly composed Authorization header using AKAv1-MD5 algorithm (as described in RFC 3310 [17]); and

4) To verify that the UE announces to support the "ipsec-3gpp" security mechanism together the IPsec layer algorithms for integrity (Rel-5 onwards) and confidentiality (Rel-6 onwards) protection (as defined in 3GPP TS 33.203)according to the procedures defined in RFC 3329 [21]; and

5) To verify that the UE supports the IPsec layer algorithms for integrity (Rel-5 onwards) and confidentiality (Rel-6 onwards) protection as defined in 3GPP TS 33.203and uses the one that is preferred by the P-CSCF according to the procedures defined in RFC 3329 [21]; and

6) To verify that the UE sets up two pairs of security associations as defined in 3GPP TS 33.203 [14] clause 7 and uses those for sending the REGISTER request to authenticate itself and for sending any other subsequent request; and

7) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER sent for authentication, the UE stores the default public user identity and information about barred user identities; and

8) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER sent for authentication, the UE subscribes to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in RFC 3680 [22]; and

9) To verify that the UE uses the default public user identity for subscription to the registration-state event package, when the public user identity that was used for initial registration is a barred public user identity; and

10) To verify that the UE uses the stored service route for routing the SUBSCRIBE sent; and

11) To verify that after receiving a valid 200 OK response from S-CSCF to the SUBSCRIBE sent for registration event package, the UE maintains the generated dialog; and

12) To verify that after receiving a valid NOTIFY for the registration event package, the UE will update and store the registration state of the indicated public user identities accordingly (as specified in RFC 3680 [22] clause 5); and

13) To verify that the UE responds the received valid NOTIFY with 200 OK.

8.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1-11) Execute the generic test procedure in Annex C.2 up to the last step.

NOTE: This test case shall be run twice in order to test that the UE correctly supports both HMAC-MD5-96 and HMAC-SHA-1-96 algorithms. For each test round the name of the corresponding algorithm shall be configured into px_IMS_IpSecAlgorithm PIXIT.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-11			Steps defined in C.2	IMS Registration

8.1.5 Test requirements

If the UICC card equipped to the UE contains ISIM, the UE must read the following parameters from ISIM (instead of deriving them from USIM) and use they for the REGISTER requests:

- the private user identity; and
- the temporary public user identity; and
- the home network domain name.

Step 3: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5 the UE sends another REGISTER request as follows:

a) the UE sets up the temporary set of security associations between the ports announced in Security-Client header (UE) in the REGISTER request and Security-Server header (SS) in the 401 Unauthorized response; and

b) the UE uses the most preferred mechanism and algorithm returned by the SS and supported by the UE for the temporary set of security associations; and

c) the UE uses IK derived from RAND as the shared key for integrity and confidentiality protection (if the UE supports IPSec ESP confidentiality protection) for the temporary set of security associations; and

d) the UE sends the second REGISTER over the temporary set of security associations; and

Step 5: SS shall check that, in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.3, the UE sends a SUBSCRIBE request for registration event package over the newly established set of security associations.

NOTE: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header (within any of the request sent by the UE), then SS has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association (or to the unprotected port in the initial REGISTER).

8.2 User Initiated Re-Registration

8.2.1 Definition

Test to verify that the UE can re-register a previously registered public user identity at any time. This process is described in 3GPP TS 24.229 [10], clause 5.1.1.4.

8.2.2 Conformance requirement

[TS 24.229, clause 5.1.1.4.1]:

The UE can perform the reregistration of a previously registered public user identity bound to any one of its contact addresses and the associated set of security associations or TLS sessions at any time after the initial registration has been completed.

The UE can perform the reregistration of a previously registered public user identity over any existing set of security associations or TLS session that is associated with the related contact address.

The UE can perform the reregistration of a previously registered public user identity via an initial registration as specified in subclause 5.1.1.2, when binding the previously registered public user identity to new contact address.

The UE can perform registration of additional public user identities at any time after the initial registration has been completed. The UE shall perform the registration of additional public user identities either:

- over the existing set of security associations or TLS sessions, if appropriate to the security mechanism in use, that is associated with the related contact address; or

- via an initial registration as specified in subclause 5.1.1.2.

The UE can fetch bindings as defined in RFC 3261 at any time after the initial registration has been completed. The procedure for fetching bindings is the same as for a reregistration except that the REGISTER request does not contain a Contact header field.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister an already registered public user identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 or when the UE needs to modify the ICSI values that the UE intends to use in a g.3gpp.icsi-ref media feature tag or IARI values that the UE intends to use in the g.3gpp.iari-ref media feature tag.

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203, established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep;

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 2: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep, towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229, clause 5.1.1.4.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

  - the "username" header field parameter set to the value of the private user identity;

  - the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;

  - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

  - the "nonce" header field parameter, set to last received nonce value; and

  - the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203.

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

b) additionally for the Contact header field, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;

d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 and RFC 3329; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

a) set the security association lifetime associated with this contact address and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

NOTE 4: If the UE receives Authentication-Info, it will proceed as described in RFC 3310.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.1.4.1 and 5.1.1.4.2.

8.2.3 Test purpose

1) To verify that the UE can re-register a previously registered public user identity at either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less; and

2) Extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration; and

3) To verify that the UE populates the header field in the REGISTER request with From, To, Via, Contact, Authorization, Expires, Security-Client, Security-verify, Supported, and P-Access-Network-Info headers; and

4) Upon receiving 200 OK for REGISTER, the UE shall store the new expiration time of the registration for this public user identity, the list of URIs contained in the P-Associated-URI header value and use these values in the next re-register request.

8.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1-8C) The same procedure as in Annex C.2 is used with the exception that the SS sets the expiration time to 120 seconds in Step 4.

9) Before half of the time has expired from the initial registration SS receives re-register message request with the From, To, Via, Contact, Authorization, Expires, Security-Client, Security-verify, Supported, and P-Access-Network-Info header fields.

10) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1200 seconds) of the registration for this public user identity.

11) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

12) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1800 seconds) of the registration for this public user identity.

13) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

14) SS responds to the REGISTER request with valid 200 OK response. SS shall populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8C			Messages 1-11 of Annex C.2	The same messages as in Annex C.2 are used with the exception that in Step 7 of C.2, the SS responds with 200 OK indicating 120 seconds expiration time.
9	→		REGISTER	The SS receives REGISTER from the UE 60 seconds before the expiration time set in the initial registration request.
10	←		200 OK	The SS responds with 200 OK indicating 1200 seconds expiration time.
11	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 10.
12	←		200 OK	The SS responds with 200 OK indicating 1800 seconds expiration time.
13	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 12
14	←		200 OK	The SS responds with 200 OK indicating the default expiration time.

Specific Message Contents

Messages in Step 1-8C

Messages in Step 1-8C are the same as those specified in Annex C.2 with the following exception for the 200 OK for REGISTER in Step 7 of C.2:

Use the default message “200 OK for REGISTER” in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	120

REGISTER (Step 9)

Use the default message “REGISTER” in annex A.1.1 with conditions A2 "Subsequent REGISTER sent over security associations" and A17 "UE initiated IMS re-registration or de-registration" and with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, shall be different than in step 3
spi-s	new SPI number of the inbound SA at the protected server port, shall be different than in step 3
port-c	new protected client port, shall be different than in step 3
port-s	Same value as in the previous REGISTER

200 OK for REGISTER (Step 10)

Use the default message “200 OK for REGISTER” in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	1200

REGISTER (Step 11)

Use the default message “REGISTER” in annex A.1.1 with conditions A2 "Subsequent REGISTER sent over security associations" and A17 "UE initiated IMS re-registration or de-registration" and with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, shall be different than in step 3 but may or may not be the same as in step 9
spi-s	new SPI number of the inbound SA at the protected server port, shall be different than in step 3 but may or may not be the same as in step 9
port-c	new protected client port, shall be different than in step 3 but may or may not be the same as in step 9
port-s	Same value as in the previous REGISTER

200 OK for REGISTER (Step 12)

Use the default message “200 OK for REGISTER” in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	1800

REGISTER (Step 13)

Use the default message “REGISTER” in annex A.1.1 with conditions A2 "Subsequent REGISTER sent over security associations" and A17 "UE initiated IMS re-registration or de-registration" and with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, shall be different than in step 3 but may or may not be the same as in step 9 or step 11
spi-s	new SPI number of the inbound SA at the protected server port, shall be different than in step 3 but may or may not be the same as in step 9 or step 11
port-c	new protected client, shall be different than in step 3 but may or may not be the same as in step 9 or step 11
port-s	Same value as in the previous REGISTER

200 OK for REGISTER (Step 14)

Use the default message “200 OK for REGISTER” in annex A.1.3.

8.2.5 Test requirements

1. The UE shall in step 9 send the REGISTER request within 60 seconds from the time instant that it receives 200 OK in step 4 from the SS.
2. The UE shall in step 11 send the REGISTER request within 600 seconds from the time instant that it receives 200 OK from the SS in step 10.
3. The UE shall in step 13 send the REGISTER request within 1200 seconds from the time instant that it receives 200 OK from the SS in step 12.

8.3 Mobile Initiated Deregistration

8.3.1 Definition

Test to verify that the UE can perform a correct de-registration procedure. This process is described in 3GPP TS 24.229 [10], clause 5.1.1.6.

8.3.2 Conformance requirement

[TS 24.229, clause 5.1.1.6.1]:

The UE can deregister a public user identity that it has previously registered with its contact address at any time. The UE shall protect the REGISTER request using a security association or TLS session that is associated with contact address, see 3GPP TS 33.203, established as a result of an earlier registration, if one is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs that were using the contact addresses that is going to be deregistered and related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities. However:

- if the dialog that was established by the UE subscribing to the reg event package used the public user identity that is going to be deregistered; and
- this dialog is the only remaining dialog used for subscription to reg event package of the user, i.e. there are no other contact addresses registered with associated subscription to the reg event package of the user;

then the UE shall not release this dialog.

On sending a REGISTER request that will remove the binding between the public user identity and one of its contact addresses, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be deregistered;

b) a To header field set to the SIP URI that contains the public user identity to be deregistered;

c) a Contact header field set to the SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, and containing the Instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE supports multiple registrations, it shall include "reg-id" header field parameter as described in RFC 5626;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field;

e) a registration expiration interval value set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

h) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

For a public user identity that the UE has registered with multiple contact addresses (e.g. via different P-CSCFs), the UE shall also be able to deregister multiple contact addresses, bound to its public user identity, via single deregistration procedure as specified in RFC 3261. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a list of Contact headers. Each Contact header in the list shall contain the contact addresses that the UE wants to deregister with the "expires" parameter containing the value equal zero.

The UE can deregister all contact addresses bound to its public user identity and associated with its private user identity. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a public user identity that is being deregistered in the To header field, and a single Contact header field with value of "*" and the Expires header field with a value of "0".

NOTE 2: All entities subscribed to the reg event package of the user will be inform via NOTIFY request which contact addresses bound to the public user identity have been deregistered.

When a 401 (Unauthorized) response to a REGISTER request is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- remove all registration details relating to this public user identity and the associated contact address.
- store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 9: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

If there are no more public user identities registered with this contact address, the UE shall delete any stored media plane security mechanisms and related keys and any security associations or TLS sessions and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and all security association or TLS session is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

[TS 24.229, clause 5.1.1.6.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:
   - the "username" header field parameter, set to the value of the private user identity;
   - the "realm" header field parameter, set to the value as received in the "realm" WWW-Authenticate header field parameter;
   - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
   - the "nonce" header field parameter, set to last received nonce value; and
   - the response directive, set to the last calculated response value;
b) additionally for each Contact header field and associated contact address, include the associated protected server port value in the hostport parameter;
c) additionally for the Via header field, include the protected server port value bound to the security association in the sent-by field;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

d) a Security-Client header field, set to specify the signalling plane security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 and RFC 3329; and
e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

NOTE 2: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with this contact address and its associated set of implicitly registered public user identities (i.e. no other public user identity is registered), the UE removes the security association (between the P-CSCF and the UE) that were using this contact address. Therefore further SIP signalling using this security association (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.1.6.1 and 5.1.1.6.2.

8.3.3 Test purpose

1) To verify that the UE sends a correctly composed initial REGISTER request with an expiration interval value set to 0 to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.1.6.

2) To verify that the UE sends correctly composed unsubscriptions, in case the UE unsubscribes from its event packages.

8.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services by performing the generic registration test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

0) The UE is triggered by MMI to initiate a deregistration procedure.

0A-0D) UE optionally unsubscribes from event packages it had subscribed to.

1) IMS deregistration is initiated on the UE. SS waits for the UE to send a REGISTER request, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.6.

2) SS responds to REGISTER with a correctly composed 200 OK message.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
0			Make the UE deregister from IMS	
0A-2			Steps 0A-2 defined in Annex C.30	

8.3.5 Test Requirements

SS shall check in steps 0A-0D that the UE uses headers as described in C.30 in case it unsubscribes from event packages.

SS shall check in step 1 that the de-register request sent by the UE has the headers correctly populated as per the default message "REGISTER" in annex A.1.1 condition A2, except for the headers described in 8.3.4.

8.4 Invalid behaviour- 423 Interval too brief

8.4.1 Definition

Test to verify that the UE sends another REGISTER request using a correct expiration timer when a registration attempt was rejected with a 423 (Interval Too Brief) response.

8.4.2 Conformance requirement

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.1.2.1.

8.4.3 Test purpose

To verify that after receiving a valid 423 (Interval Too Brief) response to the REGISTER request, the UE sends another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

8.4.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test procedure

1 IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request.

2 SS responds to the initial REGISTER request with a 423 (Interval Too Brief) response.

3 SS waits for the UE to send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

4 Continue test execution with the Generic test procedure in Annex C.2, step 5, with the modifications listed below.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		423 Interval Too Brief	The SS responds with a 423 (Interval Too Brief) too brief response to the REGISTER request with T value in Min-Expires header.
3	→		REGISTER	UE sends a new REGISTER request with expires parameter value set to Tmod (equal or greater to T value in Min-Expires header of 423 (Interval Too Brief)).
4	←→		Continue with Annex C.2 step 5	Execute the Generic test procedure Annex C.2 steps 5-11 in order to get the UE in a stable registered state.

Specific Message Contents

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1 with condition A1 “Initial unprotected REGISTER”.

423 Interval Too Brief for REGISTER (Step 2)

Use the default message “423 Interval Too Brief for REGISTER” in annex A.1.7 with the following exception:

Header/param	**Value/remark**
Min-Expires	
delta-seconds	*800000* (referred to as T in the test procedure and test requirement)

REGISTER (Step 3)

Use the default message “REGISTER” in annex A.1.1 with condition A1 “Initial unprotected REGISTER” with the following exceptions:

Header/param	**Value/remark**
Contact	
expires	*800000* (referred to as Tmod in the expected sequence) (if present, see Rule 1)
Expires	(if present, see Rule 1)
delta-seconds	*800000* (referred to as Tmod in the expected sequence)
CSeq	
value	must be incremented from the previous REGISTER

Rule 1: The REGISTER request must contain either an Expires header or an expires parameter in the Contact header. If both are present the value of Expires header is not important.

Modifications to steps detailed in Appendix C.2:

REGISTER (Step 6)

Header/param	**Value/remark**
Contact	
expires	*800000* (if present)
Expires	(if present)
delta-seconds	*800000*

200 OK (Step 7)

Header/param	**Value/remark**
Contact expires	 800000

8.4.5 Test requirements

Step 3: The UE shall send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

8.5 to 8.9 Void

8.10 Initial registration using GIBA

8.10.1 Definition

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains ISIM and USIM applications or only USIM application. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered and subscribing the registration event package for the registered default public user identity, i.e. the UE uses GIBA as security scheme.

8.10.2 Conformance requirement

[TS 24.229 Rel-8, clause 5.1.1.2.1]

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4).

[TS 24.229 Rel-9, clause 5.1.1.2.1]:

…

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 4: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

[TS 24.229 Rel-10, clause 5.1.1.2.1]

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE:

   1) supports GRUU (see table A.4, item A.4/53);

   2) supports multiple registrations;

   3) has an IMEI available; or

   4) has an MEID available;

   the UE shall include a "+sip.instance" header field parameter containing the instance ID. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223 [143];

NOTE 3: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 4: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

1) if GRUU is supported, the option-tag "gruu"; and

2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

[TS 24.229, clause 5.1.1.2.6]

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support for GPRS-IMS-Bundled authentication.

b) the Security-Client header field as defined in RFC 3329 shall not be included;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

[TS 24.229, clause 5.1.1.3]

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680.

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

[TS 24.229 Rel-8, clause 5.1.1.3]

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

g) a Contact header field set to contain:

- the same IP address or FQDN, and if multiple registrations is supported, its instance ID ("+sip.instance" header field parameter) and an "ob" SIP URI parameter as described in RFC 5626 [92];

- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; and

- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial REGISTER request.

[TS 24.229 Rel-9, clause 5.1.1.3]

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) void; and

g) void.

[TS 24.229, clause 5.1.2A.1.1]

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using either a given contact address or to the registration flow and the associated contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:

a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

…

- if GPRS-IMS-Bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2.

…

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

   - if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627; or

   - if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627; or

   - otherwise, a SIP URI containing the contact address of the UE;

NOTE 7: The above items are mutually exclusive.

2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626;

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841, the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and

4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841, the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

…

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

[TS 24.341, clause 5.3.2.2]

a) On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

TS 24.229 [10] clauses 5.1.1.2.1, 5.1.1.2.6, 5.1.1.3, 5.1.2A.1.2 and TS 24.341 [90] clause 5.3.2.2.

8.10.3 Test purpose

1) To verify that UE correctly derives a temporary public user identity from the IMSI parameter.

2) Void

3) To verify that the UE sends a correctly composed initial REGISTER request.

4) To verify that after receiving a 200 OK response, the UE subscribes to the reg event package.

5) To verify that the UE responds the received NOTIFY with 200 OK.

8.10.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2a up to step 3.

SS is configured with the IMSI, the home domain name, public and private user identities and the currently assigned IP address. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test procedure

1) The UE initiates IMS registration indicating support of GIBA. SS waits for the UE to send an initial REGISTER request.

2) The SS responds to the REGISTER request with a 200 OK response,

3) The SS waits for the UE to send a SUBSCRIBE request.

4) The SS responds to the SUBSCRIBE request with a 200 OK response.

5) The SS sends a valid NOTIFY request for the subscribed registration event package.

6) The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The UE sends initial registration for IMS services indicating support for GIBA procedure by not including an Authorization header field.
2	←		200 OK	The SS responds with 200 OK.
3	→		SUBSCRIBE	The UE subscribes to its registration event package.
4	←		200 OK	The SS responds with 200 OK.
5	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
6	→		200 OK	The UE responds with 200 OK.

NOTE: The default message contents in annex A are used.

Specific Message Contents

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1 with condition A3 "REGISTER for the case UE supports GIBA" and condition A6 “The UE supports SM-over-IP receiver” (if UE supports SM-over-IP receiver marked as yes).

200 OK for REGISTER (Step 2)

Use the default message “200 OK for REGISTER” in annex A.1.3 with condition A2 “GIBA”.

SUBSCRIBE (Step 3)

Use the default message “SUBSCRIBE for reg-event package” in annex A.1.4 with condition A2 “GIBA”.

200 OK for SUBSCRIBE (Step 4)

Use the default message “200 OK for SUBSCRIBE” in annex A.1.5 with condition A2 “GIBA”.

NOTIFY (Step 5)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with condition A2 “GIBA”.

200 OK for NOTIFY (Step 6)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

8.10.5 Test requirements

The UE shall send requests and responses as described in clause 8.10.4.

8.11 Initial registration using IMS AKA and GIBA against a network with GIBA support only

8.11.1 Definition

Test to verify that the UE can correctly register to IMS services in a network with support for GIBA only, when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing the registration event package for the registered default public user identity.

8.11.2 Conformance requirement

[TS 24.229, clause 5.1.1.2.1]

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

[TS 24.229 Rel-8, clause 5.1.1.2.1]

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4).

[TS 24.229 Rel-9, clause 5.1.1.2.1]

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 4: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

[TS 24.229 Rel-10, clause 5.1.1.2.1]

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE:

   1) supports GRUU (see table A.4, item A.4/53);

   2) supports multiple registrations;

   3) has an IMEI available; or

   4) has an MEID available;

   the UE shall include a "+sip.instance" header field parameter containing the instance ID. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223;

NOTE 3: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 4: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

    1) if GRUU is supported, the option-tag "gruu"; and

    2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

[TS 24.229, clause 5.1.1.2.2]

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

    - the "username" header field parameter, set to the value of the private user identity;

    - the "realm" header field parameter, set to the domain name of the home network;

    - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

    - the "nonce" header field parameter, set to an empty value; and

    - the "response" header field parameter, set to an empty value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the port values see 3GPP TS 33.203.

b) additionally for the Contact header field, if the REGISTER request is protected by a security association, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field; and

d) a Security-Client header field set to specify the signalling plane security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203. The syntax of the parameters needed for the security association setup is specified in annex H of 3GPP TS 33.203. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329. The UE shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203, and shall announce support for them according to the procedures defined in RFC 3329.

[TS 24.229, clause 5.1.1.2.6]

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support for GPRS-IMS-Bundled authentication.

b) the Security-Client header field as defined in RFC 3329 shall not be included;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

[TS 24.229, clause 5.1.1.3]

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680.

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

[TS 24.229 Rel-8, clause 5.1.1.3]

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

g) a Contact header field set to contain:

- the same IP address or FQDN, and if multiple registrations is supported, its instance ID ("+sip.instance" header field parameter) and an "ob" SIP URI parameter as described in RFC 5626 [92];
- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; and
- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial REGISTER request.

[TS 24.229 Rel-9, clause 5.1.1.3]

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) void; and

g) void.

[TS 24.229, clause 5.1.2A.1.1]

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using either a given contact address or to the registration flow and the associated contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

…

- if GPRS-IMS-Bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2.

…

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

   - if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627; or

   - if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627; or

   - otherwise, a SIP URI containing the contact address of the UE;

NOTE 7: The above items are mutually exclusive.

2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626;

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841, the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and

4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841, the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

…

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

[TS 33.203, clause T.7]

3. ME supports both, IMS network supports GIBA security only.

   The ME shall check the smartcard application in use.

   If a SIM is in use, then it shall start with a GIBA security procedure, else it shall start with the fully compliant IMS Registration procedure.

   In the second case, the GIBA P-CSCF shall answer with a 420 (Bad Extension) failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial REGISTER request.

NOTE 2: The Proxy-Require header cannot be ignored by the P-CSCF.

   The UE shall, after receiving the error response, send a GIBA registration, i.e., shall send a new REGISTER request without the fully compliant IMS security headers.

NOTE 3: If the UE already has knowledge about the IMS network capabilities (which could for example be preconfigured in the UE), the appropriate authentication method can be chosen. The UE can use fully compliant IMS security, if the network supports this, otherwise the UE can use GIBA security.

[TS 24.341, clause 5.3.2.2]

a) On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

TS 24.229 [10] clauses 5.1.1.2.1, 5.1.1.2.2, 5.1.1.2.6, 5.1.1.3, 5.1.2A.1.2, TS 33.203 [14] clause T.7 and TS 24.341 [90] clause 5.3.2.2.

8.11.3 Test purpose

1) To verify that UE correctly derives a private user identity, a temporary public user identity and a home network domain name from the IMSI parameter in the USIM or alternatively use the values retrieved from ISIM.

2) To verify that the UE sends a correctly composed initial REGISTER request.

3) To verify that after receiving a 420 (Bad Extension) response the UE sends a correctly composed initial REGISTER request.

4) To verify that after receiving a 200 OK response, the UE subscribes to the reg event package.

5) To verify that the UE responds the received NOTIFY with 200 OK.

8.11.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3. The UE has no knowledge about the IMS network capabilities.

SS is configured with the IMSI, the home domain name, public and private user identities and the currently assigned IP address. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test procedure

1) IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request.

2) The SS responds to the REGISTER request with a 420 Bad Extension response,

3) The UE initiates IMS registration indicating support of GIBA. SS waits for the UE to send an initial REGISTER request.

4) The SS responds to the REGISTER request with valid 200 OK response,

5) The SS waits for the UE to send a SUBSCRIBE request.

6) The SS responds to the SUBSCRIBE request with a valid 200 OK response.

7) The SS sends a NOTIFY request for the subscribed registration event package.

8) The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		420 Bad Extension	The SS responds with a failure, since the option tag sec-agree in the Proxy-Require header field is not supported.
3	→		REGISTER	The UE sends initial registration for IMS services indicating support for GIBA procedure by not including an Authorization header field.
4	←		200 OK	The SS responds with 200 OK.
5	→		SUBSCRIBE	The UE subscribes to its registration event package.
6	←		200 OK	The SS responds with 200 OK.
7	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
8	→		200 OK	The UE responds with 200 OK.

NOTE: The default message contents in annex A are used.

Specific Message Contents

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1 with condition A1 "Initial unprotected REGISTER" and condition A6 “The UE supports SM-over-IP receiver” (if UE supports SM-over-IP receiver marked as yes)

420 Bad Extension (Step 2)

Use the default message “420 Bad Extension for REGISTER” in annex A.1.8

REGISTER (Step 3)

Use the default message “REGISTER” in annex A.1.1 with condition A3 "REGISTER for the case UE supports GIBA" and condition A6 “The UE supports SM-over-IP receiver” (if UE supports SM-over-IP receiver marked as yes)

200 OK for REGISTER (Step 4)

Use the default message “200 OK for REGISTER” in annex A.1.3 with condition A2 “GIBA”

SUBSCRIBE (Step 5)

Use the default message “SUBSCRIBE for reg-event package” in annex A.1.4 with condition A2 “GIBA”.

200 OK for SUBSCRIBE (Step 6)

Use the default message “200 OK for SUBSCRIBE” in annex A.1.5 with condition A2 “GIBA”

NOTIFY (Step 7)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with condition A2 “GIBA”

200 OK for NOTIFY (Step 8)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

8.11.5 Test requirements

The UE shall send requests and responses as described in clause 8.11.4.

8.12 User initiated re-registration using GIBA

8.12.1 Definition

Test to verify that the UE can re-register a previously registered public user identity at any time using GIBA as security scheme.

8.12.2 Conformance requirement

[TS 24.229, clause 5.1.1.4.1]

The UE can perform the reregistration of a previously registered public user identity bound to any one of its contact addresses and the associated set of security associations or TLS sessions at any time after the initial registration has been completed.

The UE can perform the reregistration of a previously registered public user identity over any existing set of security associations or TLS session that is associated with the related contact address.

…

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister an already registered public user identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 or when the UE needs to modify the ICSI values that the UE intends to use in a g.3gpp.icsi-ref media feature tag or IARI values that the UE intends to use in the g.3gpp.iari-ref media feature tag.

…

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent;

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 2: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

[TS 24.229, clause 5.1.1.4.6]

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support GPRS-IMS-Bundled authentication.

b) security agreement header field values as required by RFC 3329 shall not contain signalling plane security mechanisms;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.4.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

[TS 24.341, clause 5.3.2.2]

c) On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

TS 24.229 [10] clauses 5.1.1.4.1, 5.1.1.4.6 and TS 24.341 [90] clause 5.3.2.2.

8.12.3 Test purpose

1) To verify that the UE can re-register a previously registered public user identity at either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

2) Upon receiving 200 OK for REGISTER, the UE shall store the new expiration time of the registration for this public user identity.

8.12.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services. Execute the generic test procedure in annex C.2a up to step 3.

SS is configured with the IMSI, the home domain name, public and private user identities and the currently assigned IP address. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test procedure

1-6) The same procedure as in subclause 8.10.4 are used with the exception that the SS sets the expiration time to 120 seconds in Step 4.

7) Before half of the time has expired from the initial registration SS receives re-register message request with the From, To, Via, Contact, Expires, Supported, and P-Access-Network-Info header fields.

8) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1200 seconds) of the registration for this public user identity.

9) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

10) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1800 seconds) of the registration for this public user identity.

11) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

12) SS responds to the REGISTER request with valid 200 OK response. SS shall populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-6			Messages in Initial Registration Test case (subclause 8.10.4)	The same messages as in subclause 8.10.4 are used with the exception that in Step 4, the SS responds with 200 OK indicating 120 seconds expiration time.
7	→		REGISTER	The SS receives REGISTER from the UE 60 seconds before the expiration time set in the initial registration request.
8	←		200 OK	The SS responds with 200 OK indicating 1200 seconds expiration time.
9	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 8.
10	←		200 OK	The SS responds with 200 OK indicating 1800 seconds expiration time.
11	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 10
12	←		200 OK	The SS responds with 200 OK indicating the default expiration time.

Specific Message Contents

Messages in Step 1-6

Messages in Step 1-6 are the same as those specified in subclause 8.10.4 with the following exception for the 200 OK for REGISTER in Step 4:

Use the default message "200 OK for REGISTER" in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	120

REGISTER (Step 7)

Use the default message "REGISTER" in annex A.1.1 with condition A3 "REGISTER for the case UE supports GIBA" and condition A6 "The UE supports SM-over-IP receiver" (if UE supports SM-over-IP receiver marked as yes).

200 OK for REGISTER (Step 8)

Use the default message "200 OK for REGISTER" in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	1200

REGISTER (Step 9)

Use the default message "REGISTER" in annex A.1.1 with condition A3 "REGISTER for the case UE supports GIBA" and condition A6 "The UE supports SM-over-IP receiver" (if UE supports SM-over-IP receiver marked as yes).

200 OK for REGISTER (Step 10)

Use the default message "200 OK for REGISTER" in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	1800

REGISTER (Step 11)

Use the default message “REGISTER” in annex A.1.1 with condition A3 “REGISTER for the case UE supports GIBA” and condition A6 “The UE supports SM-over-IP receiver” (if UE supports SM-over-IP receiver marked as yes).

200 OK for REGISTER (Step 12)

Use the default message “200 OK for REGISTER” in annex A.1.3.

8.12.5 Test requirements

The UE shall send requests and responses as described in clause 8.12.4

8.13 User initiated de-registration using GIBA

8.13.1 Definition

Test to verify that the UE can perform a correct de-registration procedure using GIBA as security scheme. This process is described in 3GPP TS 24.229 [10], clause 5.1.1.6.

8.13.2 Conformance requirement

[TS 24.229, clause 5.1.1.6.1]

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

…

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

…

On sending a REGISTER request that will remove the binding between the public user identity and one of its contact addresses, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be deregistered;

b) a To header field set to the SIP URI that contains the public user identity to be deregistered;

c) a Contact header field set to the SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, and containing the Instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE supports multiple registrations, it shall include "reg-id" header field parameter as described in RFC 5626;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field;

e) a registration expiration interval value set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

h) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

For a public user identity that the UE has registered with multiple contact addresses (e.g. via different P-CSCFs), the UE shall also be able to deregister multiple contact addresses, bound to its public user identity, via single deregistration procedure as specified in RFC 3261. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a list of Contact headers. Each Contact header in the list shall contain the contact addresses that the UE wants to deregister with the "expires" parameter containing the value equal zero.

The UE can deregister all contact addresses bound to its public user identity and associated with its private user identity. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a public user identity that is being deregistered in the To header field, and a single Contact header field with value of "*" and the Expires header field with a value of "0".

NOTE 2: All entities subscribed to the reg event package of the user will be inform via NOTIFY request which contact addresses bound to the public user identity have been deregistered.

[TS 24.229, clause 5.1.1.6.6]

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support GPRS-IMS-Bundled authentication.

b) the Security-Verify header field and the Security-Client header field values as defined by RFC 3329 shall not contain signalling plane security mechanisms;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be deregistered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be deregistered;

e) for each Contact header field and associated contact address include the associated unprotected port value (where the UE was expecting to receive mid-dialog requests); and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

[TS 24.341, clause 5.3.2.2]

b) On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

TS 24.229 [10] clauses 5.1.1.6.1, 5.1.1.6.6 and TS 24.341 [90] clause 5.3.2.2.

8.13.3 Test purpose

1) To verify that the UE sends an initial REGISTER request with an expiration interval value set to 0.

2) To verify that the UE sends correctly composed unsubscriptions, in case the UE unsubscribes from its event packages.

8.13.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. Execute the generic test procedure in annex C.2a.

SS is configured with the IMSI, the home domain name, public and private user identities and the currently assigned IP address. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test procedure

0) The UE is triggered by MMI to initiate a deregistration procedure.

0A-0D) UE optionally unsubscribes from event packages it had subscribed to.

1) IMS deregistration is initiated on the UE. SS waits for the UE to send a REGISTER request, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.6

2) SS responds to REGISTER with a correctly composed 200 OK message.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
0			Make the UE deregister from IMS	
0A-2			Steps 0A-2 defined in Annex C.30	

8.13.5 Test requirements

SS shall check in step 1 that the de-register request sent by the UE has the headers correctly populated as per the default message “REGISTER” in annex A.1.1 condition A3, except for the headers described in 8.13.4.

8.14 Initial registration for three implicit registration sets

8.14.1 Definition

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains ISIM application with multiple IMS public user identities (IMPU) belonging to three different implicit registration sets. Test case verifies that the UE is able to register the registration sets on parallel.

8.14.2 Conformance requirement

[TS 24.229, clause 5.1.1.1A]:

The ISIM shall always be used for authentication to the IM CN subsystem, if it is present, as described in 3GPP TS 33.203.

The ISIM is preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one or more public user identities; and
- the home network domain name used to address the SIP REGISTER request

The first public user identity in the list stored in the ISIM is used in emergency registration requests.

[TS 24.229, clause 5.1.1.2.1]:

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.1.1A and 5.1.1.2.1

8.14.3 Test purpose

1) To verify that UE is able to register three different IMS public user identities (IMPU), as found from ISIM, belonging to three different implicit registration sets.

8.14.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is equipped with a UICC that contains both ISIM and USIM applications. UE is not registered to IMS services, but has an active PDP context/ established EPS default bearer context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

Test procedure

1) If the UE supports automatic consecutive registration of multiple SIP URI IMPUs the UE is made to register all implicit registration sets for the IMPUs found on ISIM otherwise if the supports manual registration of multiple SIP URIs IPMUs the UE is triggered to register one of the SIP URI IMPUs.

2) The UE executes the procedures of annex C.2 for context activation and subsequent IMS registration. The registration event sent by the SS indicates only that IMPU to have been registered, which was explicitly registered by the UE.

3) If the UE does not support automatic consecutive registration of multiple SIP URI IMPUs and supports manual registration of multiple SIP URIsIMPUs the UE is triggered to register another SIP URI IMPU.

4) The UE initiates another registration procedure of annex C.23, in order to register a second implicit registration set. The registration event sent by the SS indicates the rest of the two IMPUs within ISIM to have been registered.

5) If the UE does not support automatic consecutive registration of multiple SIP URI IMPUs and supports manual registration of multiple SIP URIs IMPUs the UE is triggered to register a third SIP URI IMPU.

6) The UE initiates a third registration procedure of annex C.23, in order to register a third implicit registration set. The registration event sent by the SS indicates all the three IMPUs within ISIM to have been registered.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				Registration of first IMPU is triggered either automatically or manually.
2			Steps defined in annex C.2	EPS bearer or PDP context activation and subsequent IMS registration for the first implicit registration set by the UE
3				Registration of second IMPU is triggered either automatically or manually.
4			Steps defined in annex C.23	IMS registration for the second implicit registration set
5				Registration of second IMPU is triggered either automatically or manually.
6			Steps defined in annex C.23	IMS registration for the third implicit registration set

Specific Message Contents

NOTIFY (within step 2)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with the following exceptions:

Header/param	*Cond*	Value/remark	Rel	Reference
Message-body	A3	<?xml version=”1.0” encoding="UTF-8"?> <reginfo xmlns=”urn:ietf:params:xml:ns:reginfo” version=”0” state=”full”> <registration aor=”<IMPU registered by the UE>” id=”a100” state=”active”> <contact id=”980” state=”active” event=”registered”> <uri>same value as in Contact header of REGISTER request</uri> </contact> </reginfo>		RFC 3680 [22]
	A4	<?xml version=”1.0” encoding="UTF-8"?> <reginfo xmlns=”urn:ietf:params:xml:ns:reginfo” xmlns:gr="urn:ietf:params:xml:ns:gruuinfo" version=”0” state=”full”> <registration aor=”<IMPU registered by the UE>” id=”a100” state=”active”> <contact id=”980” state=”active” event=”registered” callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> <gr:pub-gruu uri="public GRUU for the UE"/> <gr:temp-gruu uri="temporary GRUU for the UE" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> </reginfo>		RFC 5628 [62]

NOTIFY (within step 4)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with the following exceptions:

- The version of the reginfo to be 1 instead of 0.
- The state of the reginfo to be “partial” instead of “full”

- Within the reginfo XML structure there is only one single <registration> element for the IMPU registered within step 4 by the UE

NOTIFY (within step 6)

Use the default message "NOTIFY for reg-event package" in annex A.1.6 with the following exceptions:

- The version of the reginfo to be 2 instead of 0.
- The state of the reginfo to be "partial" instead of "full".
- Within the reginfo XML structure there is only one single <registration> element for the IMPU registered within step 6 by the UE.

Thus:

- The full registration event sent by SS after the first REGISTER from the UE indicates only single IMPU explicitly registered to belong to the first implicit registration set.
- The partial event sent by SS after the second REGISTER from the UE indicates second IMPUs on ISIM to have been registered.
- The partial event sent by SS after the third REGISTER from the UE indicates the third IMPUs on ISIM to have been registered.

8.14.5 Test requirements

UE shall register three implicit registration sets to which the IMPUs on ISIM have been divided.

The UE shall read the following parameters from ISIM and use them for the REGISTER requests:

- the private user identity; and
- the public user identities; and
- the home network domain name.

8.15 Refresh for ISIM parameters

8.15.1 Definition

Test to verify that the when ISIM parameter values have been updated the UE will use the new values when registering to IMS the next time.

8.15.2 Conformance requirement

[TS 24.229 Annex C.4]:

The 3GPP TS 31.102 and 3GPP TS 31.103 specify the file structure and contents for the preconfigured parameters stored on the USIM and ISIM, respectively, necessary to initiate the registration to the IM CN subsystem. Any of these parameters can be updated via Data Download or a USAT application, as described in 3GPP TS 31.111. If one or more EFs are changed and a REFRESH command is issued by the UICC, then the UE reads the updated parameters from the UICC as specified for the REFRESH command in 3GPP TS 31.111.

In case of changes to EFs, the UE is not required to perform deregistration but it shall wait for the network-initiated deregistration procedures to occur as described in subclause 5.4.1.5 unless the user initiates deregistration procedures as described in subclause 5.1.1.6. From this point onwards the normal initial registration procedures can occur.

[TS 24.229 clause 5.1.1.7]:

Upon receipt of a NOTIFY request on any dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute within the <contact> element belonging to this UE set to "rejected" or "deactivated"; or

- the state attribute set to "active" and within the <contact> element belonging to this UE, the state attribute set to "terminated" and the associated event attribute set to "rejected" or "deactivated";

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 5.1.1.2.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.1.7, annex C.4 (release 10)

8.15.3 Test purpose

1) To verify that the update of ISIM parameters related to IMS registration (and consequent REFRESH command) does not cause the UE to immediately deregister from IMS; and

2) To verify that the UE uses the updated parameter values from ISIM when registering to IMS again after the network initiated deregistration procedure

8.15.4 Method of test

Initial conditions

SS is configured with the old and new home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is equipped with a UICC that contains both ISIM and USIM applications. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step. The Request-URI of SIP REGISTER request sent by the UE contained the old home domain name and IMS identities as found from ISIM.

Test procedure

1) The UICC is made to send a REFRESH command to the UE indicating that contents of ISIM has been updated.

NOTE: The specific way to trigger the REFRESH command is a test implementation option.

2) 10 seconds after step 1 SS sends a SIP NOTIFY request in order to terminate the IMS registration.

3) UE responds the NOTIFY request with 200 OK response.

4) UE initiates a new IMS registration sequence. For SIP REGISTER request the UE uses the new values of home domain name and/or IMS identities as provided by ISIM after the update.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			REFRESH	The UICC is made to send a REFRESH command to the UE indicating that contents of ISIM has been updated.
2	←		NOTIFY	10 seconds after previous step 1 the SS sends SIP NOTIFY for registration event package, containing full registration state information, with all previously registered IMS public user identities as "terminated" and "deactivated"
3	→		200 OK	The UE responds the NOTIFY with 200 OK
4			Steps defined in annex C.2 from step 4 onwards	UE initiates a new IMS registration sequence. For the Request-URI of SIP REGISTER request the UE uses the new value of home domain and/or IMS identities name as provided by ISIM after the update in step 1.

Specific Message Contents

NOTIFY (Step 2)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with the following exceptions:

Header/param	Value/remark
CSeq value	 2
Subscription-State substate-value expires	 *Terminated* *0*
Message-body	*<?xml version=”1.0” encoding="UTF-8"?>* *<reginfo xmlns=”urn:ietf:params:xml:ns:reginfo” version=”1” state=”full”>* <*registration aor*=”PublicUserIdentity1 (NOTE 1)” *id=”a100” state=”terminated”*> *<contact id=”980” state=”terminated” event=”deactivated”>* <*uri*>same value as in Contact header of REGISTER request<*/uri*> *</contact>* *</registration>* <*registration aor*=”AssociatedTelUri (NOTE 1)” *id=”a101” state=”terminated”*> *<contact id=”981” state=”terminated” event=”deactivated”>* <*uri*>same value as in Contact header of REGISTER request<*/uri*> *</contact>* *</registration>* <*registration aor*=”PublicUserIdentity2 (NOTE 1)” *id=”a102” state=”terminated”*> *<contact id=”982” state=”terminated” event=”deactivated”>* <*uri*>same value as in Contact header of REGISTER request<*/uri*> *</contact>* *</registration>* *</reginfo>*

NOTE 1: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI;
AssociatedTelUri is the same as used in P-Associated-URI
PublicUserId2 and PublicUserId3 are the remaining IMPUs of the P-Associated-URI header

200 OK for NOTIFY (Step 3)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

8.15.5 Test requirements

UE shall not deregister from IMS between steps 1 and 2.

In step 4 (referring to the messages defined in annex C.2) all the requests sent by the UE contain the new updated home domain name and/or IMS identities which the UE has read from ISIM after step 1.

More specifically the UE shall use the new values read from ISIM for constructing the following headers:

Request-URI: HomeDomainName, IMPU
From: IMPU
To: IMPU
Authorization: PrivateUserIdentity, HomeDomainName

8.16 User initiated re-registration - 423 Interval Too Brief

8.16.1 Definition

Test to verify that the UE can send another REGISTER request using a correct expiration timer when a reregistration attempt was rejected with a 423 (Interval Too Brief) response, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.4.1.

8.16.2 Conformance requirement

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.1.4.1

8.16.3 Test purpose

To verify that after receiving a valid 423 (Interval Too Brief) response to the REGISTER request for reregistration, the UE sends another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

8.16.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has performed the generic test procedure in Annex C.2 up to step 3.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1-8) The same procedures as in steps 4-11 of C.2 are used with the exception that the SS sets the expiration time to 120 seconds in Step 4.

9) Before half of the time has expired from the initial registration SS receives re-register message request with the From, To, Via, Contact, Authorization, Expires, Security-Client, Security-verify, Supported, and P-Access-Network-Info header fields.

10) SS responds to the re-register message request with a 423 (Interval Too Brief) response.

11) SS waits for the UE to send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

12) The SS responds to the REGISTER request with a valid 200 OK response indicating the default expiration timeout.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8	←→		Messages 3-11 of C.2	The same messages as in C.2 (steps 3-11) are used with the exception that in Step 4 (resp Step 7 in C.2), the SS responds with 200 OK indicating 120 seconds expiration time.
9	→		REGISTER	The SS receives REGISTER from the UE 60 seconds before the expiration time set in the initial registration request.
10	←		423 Interval Too Brief	The SS responds with a 423 (Interval Too Brief) too brief response to the REGISTER request with T value in Min-Expires header.
11	→		REGISTER	UE sends a new REGISTER request with expires parameter value set to Tmod (equal or greater to T value in Min-Expires header of 423 (Interval Too Brief)).
12	←		200 OK	The SS responds with 200 OK indicating the default expiration time.

Specific Message Contents

Messages in Step 1-8

Messages in Step 1-8 are the same as those specified in steps 3-11 of C.2 with the following exception for the 200 OK for REGISTER in Step 4 (resp Step 7 in C.2):

Use the default message “200 OK for REGISTER” in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	120

REGISTER (Step 9)

Use the default message “REGISTER” in annex A.1.1 with conditions A2 "Subsequent REGISTER sent over security associations" and A17 "UE initiated IMS re-registration or de-registration" and with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, shall be different than in step 3
spi-s	new SPI number of the inbound SA at the protected server port, shall be different than in step 3
port-c	new protected client port, shall be different than in step 3
port-s	Same value as in the previous REGISTER

423 Interval Too Brief for REGISTER (Step 10)

Use the default message "423 Interval Too Brief for REGISTER" in annex A.1.7 with the following exception:

Header/param	Value/remark
Min-Expires	
delta-seconds	*800000* (referred to as T in the test procedure and test requirement)

REGISTER (Step 11)

Use the default message "REGISTER" in annex A.1.1 with conditions A2 "Subsequent REGISTER sent over security associations" and A17 "UE initiated IMS re-registration or de-registration" with the following exceptions:

Header/param	Value/remark
Contact expires	 *800000* (referred to as Tmod in the expected sequence) (if present, see Rule 1)
Expires delta-seconds	(if present, see Rule 1) *800000* (referred to as Tmod in the expected sequence)
CSeq value	 must be incremented from the previous REGISTER

Rule 1: The REGISTER request must contain either an Expires header or an expires parameter in the Contact header. If both are present the value of Expires header is not important.

200 OK (Step 12)

Header/param	Value/remark
Contact expires	 *800000*

8.16.5 Test requirements

Step 11: The UE shall send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

9 Authentication

9.1 Invalid Behaviour – MAC Parameter Invalid

9.1.1 Definition

To test that the UE when receiving a 401 (Unauthorized) response with an invalid MAC value to its initial REGISTER request behaves correctly. This procedure is described in 3GPP TS 24.229 [10] clause 5.1.1.5.

9.1.2 Conformance requirement

[TS 24.229, clause 5.1.1.5.1]

Authentication is performed during initial registration. A UE can be re-authenticated during subsequent reregistrations, deregistrations or registrations of additional public user identities. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

…

[TS 24.229 Rel-12, clause 5.1.1.5.3]

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no "auts" Authorization header field parameter and an empty "response" Authorization header field parameter, i.e. no authentication challenge response;
- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the "auts" Authorization header field parameter (see 3GPP TS 33.102 [18]).

NOTE: In the case of the SQN being out of range, a "response" Authorization header field parameter can be included by the UE, based on the procedures described in RFC 3310 [49].

Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing set of security associations, if available (see 3GPP TS 33.203 [19]);
- populate a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the parameters needed for the new security association setup. These parameters shall contain new values for spi_uc, spi_us and port_uc; and
- not create a temporary set of security associations.

9.1.3 Test purpose

1) To verify that after receiving a 401 (Unauthorized) response for the initial REGISTER sent, the UE checks that the locally calculated XMAC matches the MAC parameter derived from the AUTN part of the challenge.
2) If the value of MAC derived from the AUTN part of the 401 (Unauthorized) response received by the UE does not match the value of locally calculated XMAC:
   - the UE responds with a further REGISTER indicating that the challenge has been deemed invalid; and
   - this subsequent REGISTER request contains no "auts" Authorization header field parameter and an empty "response" Authorization header field parameter, i.e. no authentication challenge response; and
   - the UE populates a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup. These parameters contain new values for spi_uc, spi_us and port_uc; and
   - the UE does not create a temporary set of security associations.

9.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but executed the generic test procedure in Annex C.2 up to step 3.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test procedure

1) IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.2

2) SS responds to the initial REGISTER request with an invalid 401 Unauthorized response, headers populated as follows:

   a) To, From, Via, CSeq, Call-ID and Content-Length headers according to RFC 3261 [15] clauses 8.2.6.2 and 20.14; and

   b) WWW-Authentication header with AKAv1-MD5 authentication challenge according to 3GPP TS 24.229 [10], clause 5.4.1.2.1 and RFC 3310 [17] clause 3; except that the MAC value in AUTN should be incorrect

   c) Security-Server header according to 3GPP TS 24.229 [10], clause 5.2.2 and RFC 3329 [21] clause 2.

3) SS waits for the UE to send a second Registration message indicating that the received 401 Unauthorized message was invalid

4) SS sends an invalid 401 Unauthorized message, same as in step 2)

5) SS waits for the UE to send a third Registration message indicating that the received 401 Unauthorized message was invalid

6) - 12) SS completes the registration procedure (to get the UE in a stable state at the end of the test case).

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		401 Unauthorized	The SS responds with an invalid AKAv1-MD5 authentication challenge with an invalid MAC value.
3	→		REGISTER	REGISTER request: - contains no AUTS directive and an empty response directive, i.e. no authentication challenge response - UE populates a new Security-Client header set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup
4	←		401 Unauthorized	The SS responds with an invalid AKAv1-MD5 authentication challenge with an invalid MAC value.
5	→		REGISTER	REGISTER request: - contains no AUTS directive and an empty response directive, i.e. no authentication challenge response - UE populates a new Security-Client header set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup
6	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
7	→		REGISTER	UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
8	←		200 OK	The SS responds with 200 OK.
9	→		SUBSCRIBE	UE subscribes to its registration event package.
10	←		200 OK	The SS responds SUBSCRIBE with 200 OK
11	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
12	→		200 OK	The UE responds the NOTIFY with 200 OK

Specific message contents

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1 with condition A1.

401 UNAUTHORIZED (Steps 2 and 4)

Use the default message “401 Unauthorized for REGISTER” in annex A.1.2 with the following exceptions:

Header/param	Value/remark
WWW-Authenticate	
nonce	Base 64 encoding of RAND and AUTN, incorrect MAC value is used to generate

REGISTER (Steps 3 and 5)

Use the default message "REGISTER" in annex A.1.1 with condition A1 with the following exceptions:

Header/param	Value/remark
CSeq	
value	The value sent in the previous REGISTER message + 1 (incremented)
Call-ID	
callid	The same value as in REGISTER in Step 1
Authorization	
response	It shall be present but empty
auth-param	If present it shall not contain the auts directive
nonce-count	value or presence of the parameter not to be checked
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, must be different from the value used in step 1 (and step 3 when in step 5)
spi-s	new SPI number of the inbound SA at the protected server port, must be different from the value used in step 1 (and step 3 when in step 5)
port-c	new protected client port needed for the setup of new pairs of security associations, must be different from the value used in step 1 (and step 3 when in step 5)

9.1.5 Test requirements

SS shall check in step 3 and 5 that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5

- the UE responds with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid; and
- sends the REGISTER request using no security associations; and
- the REGISTER request contains no AUTS directive and an empty response directive, i.e. no authentication challenge; and
- populates a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup; and
- does not create a temporary set of security associations.

9.2 Invalid Behaviour – SQN out of range

9.2.1 Definition

To test that the UE when receiving a 401 (Unauthorized) response with SQN out of range to its initial REGISTER request behaves correctly. This procedure is described in 3GPP TS 24.229 [10] clause 5.1.1.5.

To test after a failed authentication attempt that the UE when receiving a valid 401 (Unauthorized) response to its initial REGISTER request behaves correctly. This procedure is described in 24.229 [10] clause 5.1.1.5.

9.2.2 Conformance requirement

[TS 24.229, clause 5.1.1.5.1]

Authentication is performed during initial registration. A UE can be re-authenticated during subsequent reregistrations, deregistrations or registrations of additional public user identities. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

…

[TS 24.229 Rel-12, clause 5.1.1.5.3]

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no "auts" Authorization header field parameter and an empty "response" Authorization header field parameter, i.e. no authentication challenge response;

- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the "auts" Authorization header field parameter (see 3GPP TS 33.102 [18]).

NOTE: In the case of the SQN being out of range, a "response" Authorization header field parameter can be included by the UE, based on the procedures described in RFC 3310 [49].

Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing set of security associations, if available (see 3GPP TS 33.203 [19]);

- populate a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the parameters needed for the new security association setup. These parameters shall contain new values for spi_uc, spi_us and port_uc; and

- not create a temporary set of security associations.

9.2.3 Test purpose

1) To verify that after receiving a 401 (Unauthorized) response for the initial REGISTER sent, the UE checks that the SQN parameter derived from the AUTN part of the authentication challenge is within the correct range.

2) If the value of SQN derived from the AUTN part of the 401 (Unauthorized) received by the UE is out of range:

   - the UE responds with a further REGISTER indicating that the challenge has been deemed invalid; and

   - this subsequent REGISTER request contains no "auts” Authorization header field parameter and an empty "response" Authorization header field parameter, i.e. no authentication challenge response; and

   - the UE populates a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup. These parameters contain new values for spi_uc, spi_us and port_uc; and

   - the UE does not create a temporary set of security associations.

3) To verify after a failed authentication attempt if the UE receives a valid 401 (Unauthorized) message from the network in response to the Register request sent, the UE is able to perform the authentication and registration successfully.

9.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test procedure

1) IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.2

2) SS responds to the initial REGISTER request with an invalid 401 Unauthorized response, headers populated as follows:

   a) To, From, Via, CSeq, Call-ID and Content-Length headers according to RFC 3261 [15] clauses 8.2.6.2 and 20.14; and

   b) WWW-Authentication header with AKAv1-MD5 authentication challenge according to 3GPP TS `24.229 [10], clause 5.4.1.2.1 and RFC 3310 [17] clause 3; except that the SQN value in AUTN should be out of range

   c) Security-Server header according to 3GPP TS 24.229 [10], clause 5.2.2 and RFC 3329 [21] clause 2.

3) SS waits for the UE to send a second Registration message indicating that the received 401 Unauthorized message was invalid

4) SS sends a valid 401 Unauthorized message to the UE

5) SS waits for the UE to send a Registration request using the temporary set of security associations to protect the message. The Registration request shall contain the valid answer to the authentication challenge in 401 Unauthorized sent in the previous step

6) Continue test execution with the Generic test procedure in Annex C.2, step 7, sent over the same temporary set of security associations that the UE used for sending the REGISTER request

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		401 Unauthorized	The SS responds with an invalid AKAv1-MD5 authentication challenge with SQN out of range.
3	→		REGISTER	REGISTER request: - contains AUTS directive - UE populates a new Security-Client header set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup.
4	←		401 Unauthorized	This is a valid 401 (Unauthorized) message.
5	→		REGISTER	Message is sent using the temporary set of security associations to protect the message. Contains the valid answer to the authentication challenge sent in the 401 (Unauthorized) message.
6	←→		Continue with Annex C.2 step 7	Execute the Generic test procedure Annex C.2 steps 7-11 in order to get the UE in a stable registered state.

Specific message contents

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1 with condition A1.

401 UNAUTHORIZED (Step 2)

Use the default message “401 Unauthorized for REGISTER” in annex A.1.2 with the following exceptions:

Header/param	Value/remark
WWW-Authenticate	
nonce	Base 64 encoding of RAND and AUTN, generated with SQN out of range with the AMF information field set to $AMF_{RESYNCH}$ value to trigger SQN re-synchronisation procedure in test ISIM/USIM, see TS 34.108 clause 8.1.2.2.

REGISTER (Step 3)

Use the default message “REGISTER” in annex A.1.1 with condition A1 with the following exceptions:

Header/param	Value/remark
CSeq	
value	The value sent in the previous REGISTER message + 1 (incremented)
Call-ID	
callid	The same value as in REGISTER in Step 1
Authorization	
nonce	Same value as the opaque value in the previous 401 UNAUTHORIZED message
opaque	Same value as the opaque value in the previous 401 UNAUTHORIZED message
response	parameter may exist, but value not to be checked
auth-param	auts= “auts-value”, auts-value not to be checked
nonce-count	value or presence of the parameter not to be checked
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, must be different from the value used in step 1
spi-s	new SPI number of the inbound SA at the protected server port, must be different from the value used in step 1
port-c	new protected client port needed for the setup of new pairs of security associations, must be different from the value used in step 1

REGISTER (Step 5)

Use the default message “REGISTER” in annex A.1.1 with condition A2.

9.2.5 Test requirements

SS shall check in step 3 that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5

- the UE responds with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid; and
- sends the REGISTER request using no security associations; and
- the REGISTER request contains "auts” Authorization header field parameter; and
- populates a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup; and
- does not create a temporary set of security associations.

SS shall check in step 5 that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5

- the UE sets up the temporary set of security associations between the ports announced in Security-Client header (UE) in the REGISTER request and Security-Server header (SS) in the 401 Unauthorized response; and
- sends the Registration request using the temporary set of security associations to protect the message.

10 Subscription

10.1 Invalid Behaviour – 503 Service Unavailable

10.1.1 Definition

Test to verify that when the UE receives a 503 (Service Unavailable) response to a SUBSCRIBE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents. This can happen when the server is temporarily unable to process the request due to a temporary overloading or maintenance of the server.

10.1.2 Conformance requirement

[TS 24.229, clause 5.1.2.2]

If the UA receives a 503 (Service Unavailable) response to an initial SUBSCRIBE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.2.2.

10.1.3 Test purpose

To verify that after receiving a 503 (Service Unavailable) response to a SUBSCRIBE request, containing a Retry-After header, the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents. This can happen when the server is temporarily unable to process the request due to a temporary overloading or maintenance of the server.

10.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to step 7 or C.2a (GIBA only) up to step 5.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

1) The UE sends a SUBSCRIBE request over the established security associations.
2) The SS responds to the SUBSCRIBE request with a 503 (Service Unavailable) response with the Retry-After header with period set to T, indicating how long the service is expected to be unavailable to the requesting client.
3) The SS waits for the period of time T defined in the Retry-After header, to check that the UE does not try to SUBSCRIBE for the registration event during this period.

4) The UE sends a new SUBSCRIBE request.

5) Continue test execution with the Generic test procedure in Annex C.2 or C.2a (GIBA only), step 9.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		SUBSCRIBE	UE subscribes to its registration event package.
2	←		503 Service Unavailable	The SS responds with 503 response containing a Retry-After header with period set to T.
3				SS waits for Time T to check that the UE does not re-attempt the request.
4	→		SUBSCRIBE	UE reattempts to subscribe to its registration event package.
5	←→		Continue with Annex C.2 step 9	Execute the Generic test procedure Annex C.2 steps 9-11 in order to get the UE in a stable registered state.

NOTE: The default messages contents in annex A are used with condition "IMS security " or "GIBA" when applicable

Specific Message Contents

SUBSCRIBE (Step 1)

Use the default message "SUBSCRIBE for reg-event package" in annex A.1.4.

503 Service Unavailable response (Step 2)

Use the default message "503 Service Unavailable" in annex A.4.2.

SUBSCRIBE (Step 4)

Use the default message "SUBSCRIBE for reg-event package" in annex A.1.4 with the following exception:

Header/param	Value/remark
Call-ID	
callid	value different from the previous SUBSCRIBE request

10.1.5 Test requirements

Step 3: The UE shall not automatically reattempt the request during the period duration T.

Step 4: The UE reattempts to send a SUBSCRIBE request for registration event package.

11 Notification

11.1 Network-initiated deregistration

11.1.1 Definition

Test to verify that the UE can correctly process the network initiated deregistration request.

11.1.2 Conformance requirement

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute within the <contact> element belonging to this UE set to "rejected" or "deactivated"; or

- the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 5.1.1.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

Upon receipt of a NOTIFY request, the UE shall delete the security associations towards the P-CSCF either:

- if all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header contains the value of "terminated"; or

- if each <registration> element that was registered by this UE has either the state attribute set to "terminated", or the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated".

The UE shall delete these security associations towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the received NOTIFY request terminates.

NOTE 1: Deleting a security association is an internal procedure of the UE and does not involve any SIP procedures.

NOTE 2: If the security association towards the P-CSCF is removed, then the UE considers the subscription to the reg event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").

Early IMS security:

NOTE 1: Early IMS security does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure

Reference(s)

3GPP TS 24.229 [10], clause 5.1.1.7, 3GPP TR 33.978 [59], clause 6.2.3.1.

11.1.3 Test purpose

To verify that UE will not try registration after getting a NOTIFY with all <registration> element(s) set to "terminated" and "rejected".

11.1.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

1) SS sends UE a NOTIFY request for the subscribed registration event package, indicating that registration for all the previously registered user identities has been terminated and that new registration shall not be performed. Request is sent over the existing security associations between SS and UE.

2) SS waits for the UE to respond the NOTIFY with 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing full registration state information, with all previously registered public user identities "terminated" and "rejected"
2	→		200 OK	The UE responds the NOTIFY with 200 OK

NOTE: The default messages contents in annex A are used with condition “IMS security” or “GIBA” when applicable.

Specific Message Contents

NOTIFY (Step 1)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with the following exceptions:

Header/param	Value/remark
CSeq value	 2
Subscription-State substate-value expires	 *terminated* *0*
Message-body	<?xml version="1.0 encoding="UTF-8"?> <reginfo xmlns=”urn:ietf:params:xml:ns:reginfo” version=”1” state=”full”> <registration aor=”PublicUserIdentity1 (NOTE 1)” id=”a100” state=”terminated”> <contact id=”980” state=”terminated” event=”rejected”> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor=”AssociatedTelUri (NOTE 1)” id=”a101” state=”terminated”> <contact id=”981” state=”terminated” event=”rejected”> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor=”PublicUserIdentity2 (NOTE 1)” id=”a102” state=”terminated”> <contact id=”982” state=”terminated” event=”rejected”> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor=”PublicUserIdentity3 (NOTE 1)” id=”a103” state=”terminated”> <contact id=”983” state=”terminated” event=”rejected”> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration></reginfo>

NOTE 1: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI;
AssociatedTelUri is the same as used in P-Associated-URI
PublicUserId2 and PublicUserId3 are the remaining IMPUs of the P-Associated-URI header

200 OK for NOTIFY (Step 2)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

11.1.5 Test requirements

Step 2: SS shall check that the UE sends the 200 OK response over the existing set of security associations.

SS shall check that terminal does not try to send a REGISTER message after sending 200 OK. Waiting period of one minute is sufficient.

11.2 Network initiated re-authentication

11.2.1 Definition

Test to verify that the UE can correctly process a network initiated re-authentication request and re-authenticate the user before the registration expires, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5A.

11.2.2 Conformance requirement

At any time, the UE can receive a NOTIFY request carrying information related to the reg event package (as described in subclause 5.1.1.3). If:

- the state attribute in any of the <registration> elements is set to "active";
- the value of the <uri> sub-element inside the <contact> sub-element is set to the Contact address that the UE registered; and
- the event attribute of that <contact> sub-element(s) is set to "shortened";

the UE shall:

1) use the expires attribute of the <contact> sub-element that the UE registered to adjust the expiration time for that public user identity; and
2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4, if required.

NOTE: When authenticating a given private user identity, the S-CSCF will only shorten the expiry time within the <contact> sub-element that the UE registered using its private user identity. The <contact> elements for the same public user identity, if registered by another UE using different private user identities remain unchanged. The UE will not initiate a reregistration procedure, if none of its <contact> sub-elements was modified.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.1.5A.

11.2.3 Test purpose

1) To verify that UE adjusts the expiration time for a public user identity as indicated within the received NOTIFY related to reg event package; and
2) To verify that the UE will start the re-authentication procedures at the appropriate time before the registration expires.

11.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services by executing the generic test procedure in Annex C.2 up to the last step.. The expiration time for the registration must be at least 600 seconds. Security associations have been set up between UE and the SS.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1) SS sends UE a NOTIFY request for the subscribed registration event package, indicating the shortened expiration time as 60 seconds. Request is sent over the existing security associations between SS and UE.

2) SS waits for the UE to respond the NOTIFY with 200 OK response.

3) SS waits for the UE send a REGISTER request 30 seconds before the expected new expiration time.

4) SS responds to the REGISTER request with a valid 401 Unauthorized response, headers populated according to the 401 response common message definition.

5) SS waits for the UE to set up a new set of security associations and send another REGISTER request, over those security associations.

6) The SS responds with 200 OK over the new security association

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing partial registration state information, indicating shortened expiration time (60 seconds) for the registered public user identity in the XML body.
2	→		200 OK	The UE responds the NOTIFY with 200 OK.
3	→		REGISTER	UE re-registers the user 30 seconds before the expected expiration.
4	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
5	→		REGISTER	UE completes the security negotiation procedures, sets up a new temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
6	<-		200 OK	The UE responds with 200 OK.

Specific Message Contents

NOTIFY (Step 1)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with the following exceptions:

Header/param	Cond	Value/remark
CSeq		
value		2
Message-body		
	NOT A1	<?xml version=”1.0” encoding="UTF-8"?> <reginfo xmlns=”urn:ietf:params:xml:ns:reginfo” version=”1” state=”partial”> <registration aor=” PublicUserIdentity1 (NOTE 1)” id=”a100” state=”active”> <contact id=”980” state=”active” event=”shortened” expires="60"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> </reginfo>
	A1	<?xml version=”1.0” encoding="UTF-8"?> <reginfo xmlns=”urn:ietf:params:xml:ns:reginfo” xmlns:gr="urn:ietf:params:xml:ns:gruuinfo" version=”1” state=”partial”> <registration aor=” PublicUserIdentity1 (NOTE 1)” id=”a100” state=”active”> <contact id=”980” state=”active” event=”shortened” expires="60"> callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> <gr:pub-gruu uri="public GRUU associated to this aor"/> <gr:temp-gruu uri="temporary GRUU associated to this aor" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> </reginfo>

Condition	Explanation
A1	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])

NOTE 1: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI

200 OK for NOTIFY (Step 2)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

REGISTER (Step 3)

Use the default message “REGISTER” in annex A.1.1 condition A2 with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous REGISTER

401 Unauthorized for REGISTER (Step 4)

Use the default message "401 Unauthorized for REGISTER" in annex A.1.2 with the following exceptions:

Header/param	Value/remark
Security-Server	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous Security-Server headers
WWW-Authenticate	
nonce	Base 64 encoding of a new RAND and AUTN

REGISTER (Step 5)

Use the default message "REGISTER" in annex A.1.1 with condition A2.

11.2.5 Test requirements

Step 2: SS shall check that the UE sends the 200 OK response over the existing set of security associations.

Step 3: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.4 the UE sends a REGISTER request over the existing set of security associations.

12 Call Control

12.1 Void

12.2 MO Call with preconditions at both originating UE and terminating UE – 503 Service Unavailable

12.2.1 Definition

When a server is temporarily unable to process an INVITE request for an MO call with preconditions due to a temporary overloading or maintenance of the server sends a 503 Service Unavailable response. The server may indicate when the service will be available again in a Retry-After header field. This process is described in 3GPP TS 24.229 [10], clause 5.1.3.1.

12.2.2 Conformance requirement

Upon receiving a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the originating UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.3.1.

12.2.3 Test purpose

To verify that when the UE receives a 503 (Service Unavailable) response to an initial INVITE request for an MO call with preconditions containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

12.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security). UE is configured to use the precondition mechanism.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

For value of T see specific message content for 503 (Service Unavailable) message.

1-8) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 8.

9) The SS responds with a 503 (Service Unavailable) response with the Retry-After header set to T.

10) The SS waits for the UE to send an ACK to acknowledge the reception of the 503 (Service Unavailable) response.

11) SS waits for a duration of time T and checks that the UE does not reattempt sending the INVITE request. After the time T the UE may reattempt sending the INVITE request.

12) The UE may reattempt sending the INVITE request after time T.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-3			Steps 1, 2 and 3 defined in annex C.21	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
4	←		503 Service Unavailable	Including Retry-After header with period set to T
5	→		ACK	The UE acknowledges the reception of the 503 (Service Unavailable) response
6				The SS waits for a duration of time T and checks that the UE does not re-send the INVITE request
7			Step 2 defined in annex C.21	Optional

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable

Specific Message Contents

Steps 1 - 3 as specified in annex C.21

503 Service Unavailable (Step 4)

Use the default message “503 Service Unavailable” in annex A.4.2.

12.2.5 Test requirements

At step 6 the UE shall not reattempt the INVITE request before time T from the time the SS receives the ACK from the UE in step 5.

12.2a MO Call with preconditions at both originating UE and terminating UE – 504 Server Time-out

12.2a.1 Definition

When the S-CSCF is temporarily unable to process an INVITE for an MO call with preconditions as the S-CSCF does not have the user profile or does not trust the data that it has (e.g. due to restart), the S-CSCF can reject the request by returning a 504 (Server Time-out) response to the UE with specific content as specified in 3GPP TS 24.229 [10] clause 5.4.3.2. As a result the UE will initiate restoration procedures by performing an initial registration.

12.2a.2 Conformance requirement

In the event the UE receives a 504 (Server Time-out) response containing:

1) a P-Asserted-Identity header field set to a value equal to a URI:

   a) from the Service-Route header field value received during registration; or

   b) from the Path header field value received during registration; and

2) a Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the default content disposition, identified as "3gpp-alternative-service", is applied as follows:

   a) if the 504 (Server Time-out) response includes an IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element:

      a) with the <type> child element set to "restoration" (see table 7.7AA); and

      b) with the <action> child element set to "initial-registration" (see table 7.7AB);

      then the UE:

      - shall initiate restoration procedures by performing an initial registration as specified in subclause 5.1.1.2; and

- may provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.2A.1.6

12.2a.3 Test purpose

To verify that when the UE receives a 504 (Server Time-out) response to an INVITE request for an MO call with preconditions containing a P-Asserted-Identity header field set to a value equal to a URI from the Service-Route header field value received during registration and the rest of the message is set as described in [10] subclause 5.1.2A.1.6, then the UE initiates restoration procedures by performing an initial registration as specified in [10] subclause 5.1.1.2.

12.2a.4 Method of test

Initial conditions

UE contains an ISIM and USIM or only USIM application on the UICC. UE has activated a PDP context/EPS bearer, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security). UE is configured to use the precondition mechanism.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-8) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 8.

9) The SS responds with a 504 (Server Time-out) response.

10) The SS waits for the UE to send an ACK to acknowledge the reception of 504 (Server Time-out) response.

11-18) As specified in steps 4-11 annex C.2.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-2			Steps 1-2 defined in annex C.21	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
3	←		504 Server Time-out	Set as per the specific message contents.
4	→		ACK	
5-12	→		Steps 4-11 defined in annex C.2	The UE performs an initial registration.

NOTE: The default messages contents in annex A are used with condition “IMS security” or “GIBA” when applicable.

Specific Message Contents

Steps 1-2

As specified in annex C.21

504 Server Time-out (Step 3)

Use the default message “504 Server Time-out” in Annex A.4.6

ACK (Step 4)

As specified in annex A.2.7.

Steps 5-12

As specified in annex C.2.

12.2a.5 Test requirements

After step 3 the UE shall perform an initial registration.

12.2b MO Call without preconditions at both originating UE and terminating UE – 503 Service Unavailable

12.2b.1 Definition

When a server is temporarily unable to process an INVITE request for an MO call without preconditions due to a temporary overloading or maintenance of the server sends a 503 Service Unavailable response. The server may indicate when the service will be available again in a Retry-After header field. This process is described in 3GPP TS 24.229 [10], clause 5.1.3.1.

12.2b.2 Conformance requirement

[TS 24.229, clause 5.1.3.1]:

Upon receiving a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the originating UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. This SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

…

NOTE 2: If the originating UE does not use the precondition mechanism (see subclause 5.1.3.1), it will not include any precondition information in the SDP message body.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.3.1 and 6.1.2.

12.2b.3 Test purpose

To verify that when the UE receives a 503 (Service Unavailable) response to an initial INVITE request for an MO call without preconditions containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

12.2b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security). UE is configured to not use the precondition mechanism.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

For value of T see specific message content for 503 (Service Unavailable) message.

1-8) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 8.

9) The SS responds with a 503 (Service Unavailable) response with the Retry-After header set to T.

10) The SS waits for the UE to send an ACK to acknowledge the reception of the 503 (Service Unavailable) response.

11) SS waits for a duration of time T and checks that the UE does not reattempt sending the INVITE request. After the time T the UE may reattempt sending the INVITE request.

12) The UE may reattempt sending the INVITE request after time T.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-3			Steps 1, 2 and 3 defined in annex C.21f	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
4	←		503 Service Unavailable	Including Retry-After header with period set to T
5	→		ACK	The UE acknowledges the reception of the 503 (Service Unavailable) response
6				The SS waits for a duration of time T and checks that the UE does not re-send the INVITE request
7			Step 2 defined in annex C.21f	Optional

NOTE: The default messages contents in annex A are used with condition “IMS security” or “GIBA” when applicable

Specific Message Contents

Steps 1 - 3 as specified in annex C.21f

503 Service Unavailable (Step 4)

Use the default message “503 Service Unavailable” in annex A.4.2.

12.2b.5 Test requirements

At step 6 the UE shall not reattempt the INVITE request before time T from the time the SS receives the ACK from the UE in step 5.

12.2c MO Call without preconditions at both originating UE and terminating UE – 504 Server Time-out

12.2c.1 Definition

When the S-CSCF is temporarily unable to process an INVITE for an MO call without preconditions as the S-CSCF does not have the user profile or does not trust the data that it has (e.g. due to restart), the S-CSCF can reject the request by returning a 504 (Server Time-out) response to the UE with specific content as specified in 3GPP TS 24.229 [10] clause 5.4.3.2. As a result the UE will initiate restoration procedures by performing an initial registration.

12.2c.2 Conformance requirement

[TS 24.229, clause 5.1.2A.1.6]:

In the event the UE receives a 504 (Server Time-out) response containing:

1) a P-Asserted-Identity header field set to a value equal to a URI:

   a) from the Service-Route header field value received during registration; or

   b) from the Path header field value received during registration; and

2) a Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the default content disposition, identified as "3gpp-alternative-service", is applied as follows:

   a) if the 504 (Server Time-out) response includes an IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element:

      a) with the <type> child element set to "restoration" (see table 7.7AA); and

      b) with the <action> child element set to "initial-registration" (see table 7.7AB);

then the UE:

- shall initiate restoration procedures by performing an initial registration as specified in subclause 5.1.1.2; and

- may provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. This SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

…

NOTE 2: If the originating UE does not use the precondition mechanism (see subclause 5.1.3.1), it will not include any precondition information in the SDP message body.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.2A.1.6 and 6.1.2.

12.2c.3 Test purpose

To verify that when the UE receives a 504 (Server Time-out) response to an INVITE request for an MO call without preconditions containing a P-Asserted-Identity header field set to a value equal to a URI from the Service-Route header field value received during registration and the rest of the message is set as described in [10] subclause 5.1.2A.1.6, then the UE initiates restoration procedures by performing an initial registration as specified in [10] subclause 5.1.1.2.

12.2c.4 Method of test

Initial conditions

UE contains an ISIM and USIM or only USIM application on the UICC. UE has activated a PDP context/EPS bearer, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security). UE is configured to not use the precondition mechanism.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-8) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 8.

9) The SS responds with a 504 (Server Time-out) response.

10) The SS waits for the UE to send an ACK to acknowledge the reception of 504 (Server Time-out) response.

11-18) As specified in steps 4-11 annex C.2.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-2			Steps 1-2 defined in annex C.21f	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
3	←		504 Server Time-out	Set as per the specific message contents.
4	→		ACK	
5-12	→		Steps 4-11 defined in annex C.2	The UE performs an initial registration.

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable.

Specific Message Contents

Steps 1-2

As specified in annex C.21f

504 Server Time-out (Step 3)

Use the default message "504 Server Time-out" in Annex A.4.6

ACK (Step 4)

As specified in annex A.2.7.

Steps 5-12

As specified in annex C.2.

12.2c.5 Test requirements

After step 3 the UE shall perform an initial registration.

12.3 to 12.11 Void

12.12 MO MTSI Voice Call Successful with preconditions at both originating UE and terminating UE

12.12.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup and release when using IMS Multimedia Telephony with preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.12.2 Conformance requirement

[TS 24.229, clause 5.1.2A.1]:

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using a given contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:
  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and
  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

...

- if GPRS-IMS-Bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2.

...

The UE shall determine the public user identity to be used for this request as follows:

1) if a P-Preferred-Identity was included, then use that as the public user identity for this request; or

2) if no P-Preferred-Identity was included, then use the default public user identity for the security association or TLS session and the associated contact address as the public user identity for this request;

The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 6: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g. first contacted via a registration or configuration procedure).

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

   - if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627; or

   - if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627; or

   - otherwise, a SIP URI containing the contact address of the UE;

NOTE 7: The above items are mutually exclusive.

2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626;

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841, the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and

4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841, the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

...

If this is a request for a new dialog or standalone transaction and the request is related to an IMS communication service that requires the use of an ICSI then the UE:

1) shall include the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service that is related to the request in a P-Preferred-Service header field according to draft-drage-sipping-service-identification. If a list of network supported ICSI values was received as specified in 3GPP TS 24.167, the UE shall only include an ICSI value that is in the received list;

NOTE 8: The UE only receives those ICSI values corresponding to the IMS communication services that the network provides to the user.

2) may include an Accept-Contact header field containing an ICSI value (coded as specified in subclause 7.2A.8.2) that is related to the request in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 if the ICSI for the IMS communication service is known.

NOTE 9: If the UE includes the same ICSI values into the Accept-Contact header field and the P-Preferred-Service header field, there is a possibility that one of the involved S-CSCFs or an AS changes the ICSI value in the P-Asserted-Service header field, which results in the message including two different ICSI values (one in the P-Asserted-Service header field, changed in the network and one in the Accept-Contact header field).

If an IMS application indicates that an IARI is to be included in a request for a new dialog or standalone transaction, the UE shall include an Accept-Contact header field containing an IARI value (coded as specified in subclause 7.2A.9.2) that is related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841.

NOTE 10: RFC 3841 allows multiple Accept-Contact header fields along with multiple Reject-Contact header fields in a SIP request, and within those header fields, expressions that include one or more logical operations based on combinations of media feature tags. Which registered UE will be contacted depends on the Accept-Contact header field and Reject-Contact header field combinations included that evaluate to a logical expression and the relative qvalues of the registered contacts for the targeted registered public user identity. There is therefore no guarantee that when multiple Accept-Contact header fields or additional Reject-Contact header field(s) along with the Accept-Contact header field containing the ICSI value or IARI value are included in a request that the request will be routed to a contact that registered the same ICSI value or IARI value. Charging and accounting is based upon the contents of the P-Asserted-Service header field and the actual media related contents of the SIP request and not the Accept-Contact header field contents or the contact reached.

NOTE 11: The UE only includes the header field parameters "require" and "explicit" in the Accept-Contact header field containing the ICSI value or IARI value if the IMS communication service absolutely requires that the terminating UE understand the IMS communication service in order to be able to accept the session. Including the header field parameters "require" and "explicit" in Accept-Contact header fields in requests which don’t absolutely require that the terminating UE understand the IMS communication service in order to accept the session creates an interoperability problem for sessions which otherwise would interoperate and violates the interoperability requirements for the ICSI in 3GPP TS 23.228.

...

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

NOTE 13: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs and standalone transactions. The UE shall build a list of Route header field values made out of the following, in this order:

a) the P-CSCF URI containing the IP address or the FQDN learnt through the P-CSCF discovery procedures; and

b) the P-CSCF port based on the security mechanism in use:

  - if IMS AKA or SIP digest with TLS is in use as a security mechanism, the protected server port learnt during the registration procedure;

  - if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is in use as a security mechanism, the unprotected server port used during the registration procedure;

c) and the values received in the Service-Route header field saved from the 200 (OK) response to the last registration or re-registration of the public user identity with associated contact address.

[TS 24.229, clause 5.1.2A.1.2]:

The UE may use non-international formats of E.164 addresses, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

Local numbering information is sent in the Request-URI in initials requests or stand alone transaction, using one of the following formats:

1) a tel-URI, complying with RFC 3966, with a local number followed by a "phone-context" tel URI parameter value.

2) a SIP URI, complying with RFC 3261, with the "user" SIP URI parameter set to "phone"

3) a SIP URI, complying with RFC 3261 and RFC 4967, with the "user" SIP URI parameter set to "dialstring"

The actual value of the URI depends on whether user equipment performs an analysis of the dial string input by the end user or not.

[TS 24.229, clause 5.1.2A.1.5]:

When the UE uses home-local number, the UE shall include in the "phone-context" tel URI parameter the home domain name in accordance with RFC 3966.

When the UE uses geo-local number, the UE shall:

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header field into the request), include the access technology information in the "phone-context" tel URI parameter according to RFC 3966 as defined in subclause 7.2A.10; and

- if access technology information is not available to the UE (i.e., the UE cannot insert P-Access-Network-Info header field into the request), include in the "phone-context" tel URI parameter the home domain name prefixed by the "geo-local." string according to RFC 3966 as defined in subclause 7.2A.10.

When the UE uses other local numbers, than geo-local number or home local numbers , e.g. private numbers that are different from home-local number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966, e.g. if private numbers are used a domain name to which the private addressing plan is associated.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value inserted by the UE, based on implementation.

NOTE 2: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is implementation specific.

NOTE 3: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

[TS 24.229, clause 5.1.3.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

The precondition mechanism should be supported by the originating UE.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources, an originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and

- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

Upon generating an initial INVITE request using the precondition mechanism, the UE should not indicate the requirement for the precondition mechanism by using the Require header mechanism.

NOTE 2: If an UE chooses to require the precondition mechanism, i.e. if it indicates the "precondition" option tag within the Require header, the interworking with a remote UE, that does not support the precondition mechanism, is not described in this specification.

NOTE 3: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 4: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation, in case the terminating UE does not support the PRACK request (as described in RFC 3262) and does not support the UPDATE request (as described in RFC 3311).

....

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it.

[TS 24.229, clause 6.1.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,

- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566, unless the UE knows that the precondition mechanism is supported by the remote UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 and RFC 4032; and

- the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec for one or more media streams, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

[TS 26.114, clause 5.2.1]

MTSI clients in terminals offering speech communication shall support:

AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The MTSI client in terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 26.114 Rel-8, clause 6.2.2.1]:

An MTSI client offering a speech media session for narrow-band speech and/or wide-band speech should offer SDP according to the examples in clauses A.1 to A.3.

An MTSI client shall at least offer AVP for speech media streams. An MTSI client should also offer AVPF for speech media streams. RTP profile negotiation shall be done as described in clause 6.2.1a. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]:

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556. Therefore, an MTSIclient shall include the "b=RS:" and "b=RR:" fields in SDP, and shall be able to interpret them. There shall be an upper limit on the allowed RTCP bandwidth for each RTP session signalled by the MTSI client. This limit is defined as follows:

- 4 000 bps for the RS field (at media level);
- 3 000 bps for the RR field (at media level).

If the session described in the SDP is a point-to-point speech only session, the MTSI client may request the deactivation of RTCP by setting its RTCP bandwidth modifiers to zero.

GIBA:

NOTE 1: GIBA does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1, 5.1.3 and 6.1, and TS 26.114 [66], clauses 5.2.1, 6.2.2.1, 6.2.5 and 7.3.1.

12.12.3 Test purpose

1) To verify that when initiating MO call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1).

3) To verify that the UE is able to release the call.

12.12.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-14) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to14.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.21	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
13A			The UE is triggered by MMI to release the call	
14	→		BYE	The UE releases the call with BYE
15	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Steps 1 - 13 as specified in annex C.21

BYE (Step 14)

Use the default message "BYE" in annex A.2.8.

200 OK for BYE (Step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

12.12.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 14: the UE shall send a BYE request with the correct content, according to common message definitions.

12.12a MO MTSI Voice Call Successful without preconditions at both originating UE and terminating UE

12.12a.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup and release when using IMS Multimedia Telephony without preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.12a.2 Conformance requirement

As described in 12.12.2 except

[TS 24.229, Rel-14 onwards, clause 5.1.3.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

The preconditions mechanism should be supported by the originating UE.

If the precondition mechanism is disabled as specified in subclause 5.1.5A, the UE shall not use the precondition mechanism.

[TS 24.229, clause 5.1.5A]:

The precondition disabling policy indicates whether the UE is allowed to use the precondition mechanism or whether the UE is not allowed to use the precondition mechanism.

If the precondition disabling policy is not configured, the precondition disabling policy is assumed to indicate that the UE is allowed to use the precondition mechanism.

The UE may support the precondition disabling policy.

If the UE supports the precondition disabling policy, the UE may support being configured with the precondition disabling policy using one or more of the following methods:

a) the Precondition_disabling_policy node of the $EF_{IMSConfigDat}$a file described in 3GPP TS 31.102 [15C];

b) the Precondition_disabling_policy node of the $EF_{IMSConfigData}$ file described in 3GPP TS 31.103 [15B]; and

c) the Precondition_disabling_policy node of 3GPP TS 24.167 [8G].

If the UE is configured with both the Precondition_disabling_policy node of 3GPP TS 24.167 [8G] and the Precondition_disabling_policy node of the $EF_{IMSConfigData}$ file described in 3GPP TS 31.102 [15C] or 3GPP TS 31.103 [15B], then the Precondition_disabling_policy node of the $EF_{IMSConfigData}$ file shall take precedence.

NOTE: Precedence for files configured on both the USIM and ISIM is defined in 3GPP TS 31.103 [15B].

The precondition mechanism is disabled, if the UE supports the precondition disabling policy and the precondition disabling policy indicates that the UE is not allowed to use the precondition mechanism.

The precondition mechanism is enabled, if:

1) the UE does not support the precondition disabling policy; or

2) the UE supports the precondition disabling policy and the precondition disabling policy indicates that the UE is allowed to use the precondition mechanism.

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. This SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

…

NOTE 2: If the originating UE does not use the precondition mechanism (see subclause 5.1.3.1), it will not include any precondition information in the SDP message body.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.3.1, 5.1.5A and 6.1.2.

12.12a.3 Test purpose

1) To verify that when initiating MO call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that UE performs the correct exchange of SDP messages for negotiating media without using preconditions.

3) To verify that the UE is able to release the call.

12.12a.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security). UE is configured to not use the precondition mechanism.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-14) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-9			Steps 1-9 defined in annex C.21f	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
10	→		BYE	The UE releases the call with BYE
11	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Steps 1 - 9 as specified in annex C.21f.

12.13 MT MTSI speech call with preconditions at both originating UE and terminating UE

12.13.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated speech call setup when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.13.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

If local resource reservation is not required by the terminating UE andthe terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header and:

  - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

[TS 24.229, clause 6.1.1]

During session establishment procedure, and during session modification procedures, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload is included in the message because of SIP rules described in RFC 3261.

[TS 24.229, clause 6.1.3]

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, it shall set the media streams to active mode by applying the procedures described in RFC 4566 with respect to setting the direction of media streams.

…

Upon sending a SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 26.114, clause 6.2.2.1]

An MTSI client offering a speech media session for narrow-band speech and/or wide-band speech should offer SDP according to the examples in clauses A.1 to A.3.

An MTSI client shall at least offer AVP for speech media streams. An MTSI client should also offer AVPF for speech media streams. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229 [10] clauses 5.1.4.1, 6.1.1, 6.1.3, TS 26.114 [66] clause 5.2.1, 6.2.2.1, 6.2.5 and 7.3.1.

12.13.3 Test purpose

1) To verify that, when initiating MT MTSI speech call and SS needs to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

12.13.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipp5ed into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.11	MTSI MT speech call. Referred from 36.508 [94] table 4.5A.7.3-1 for a UE with E-UTRA support.

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable

Specific Message Content

None.

12.13.5 Test requirements

The UE shall send requests and responses as described in clause 12.13.4

12.13a MT MTSI speech call when remote end reserves resources before sending INVITE

12.13a.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated speech call setup when remote end reserves resources before sending INVITE. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3, 5.1.4 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.13a.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

If local resource reservation is not required by the terminating UE andthe terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header and:

  - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

[TS 24.229, clause 6.1.1]

During session establishment procedure, and during session modification procedures, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload is included in the message because of SIP rules described in RFC 3261.

[TS 24.229, clause 6.1.2]

If the UE uses the precondition mechanism (see subclause 5.1.3.1), and the desired QoS resources for one or more media streams are available at the UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value either "optional" or as specified in RFC 3312 [30] and RFC 4032 [64] for the remote segment and shall not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE.

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 26.114, clause 6.2.2.1]

An MTSI client offering a speech media session for narrow-band speech and/or wide-band speech should offer SDP according to the examples in clauses A.1 to A.3.

An MTSI client shall at least offer AVP for speech media streams. An MTSI client should also offer AVPF for speech media streams. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229 [10] clauses 5.1.4.1, 6.1.1, 6.1.2 , TS 26.114 [66] clause 5.2.1, 6.2.2.1, 6.2.5 and 7.3.1.

12.13a.3 Test purpose

1) To verify that, when initiating MT MTSI speech call and remote end does not need to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

12.13a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-6			Steps 1-6 defined in annex C.11	
7-13			Steps 9-15 defined in annex C.11	

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked Note 3: Parameters for the AMR codec are not checked

12.13a.5 Test requirements

The UE shall send requests and responses as described in clause 12.13a.4.

12.13b MT MTSI speech call Successful without preconditions at both originating UE and terminating UE

12.13b.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated speech call setup when using IMS Multimedia Telephony without preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.13b.2 Conformance requirement

same as 12.13 except

[TS 24.229, Rel-8, clause 5.1.3.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

The preconditions mechanism should be supported by the originating UE.

[TS 24.229, Rel-8, clause 5.1.4.1]:

The preconditions mechanism should be supported by the terminating UE.

If local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

...

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism;

Reference(s)

3GPP TS 24.229 [10] clauses 5.1.3.1 and 5.1.4.1.

12.13b.3 Test purpose

1) To verify that, when initiating MT MTSI speech call the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SDP contents for negotiating media without preconditions.

12.13b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipp5ed into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-6			Steps 1-6 defined in annex C.11	MTSI MT speech call. Referred from 36.508 [94] table 4.5A.7.3-1 for a UE with E-UTRA support.
7			Step 9 defined in annex C.11	The UE responds to INVITE with 180 Ringing
8-9			Step 12-13 defined in annex C.11	SS responds to INVITE with a 200 OK final response and SS acknowledges the receipt of 200 OK for INVITE.
10-11			Step 14-15 defined in annex C.11	The SS sends BYE to release the call and UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Note 1: At least one "c=" field shall be present. Note 2: The values for fmt, payload type and format are not checked Note 3: Parameters for the AMR codec are not checked

180 Ringing (Step 7)

Use the default message “180 Ringing for INVITE” in annex A.2.6 applying condition A2 (in addition to any other applicable conditions).

BYE (Step 10)

Use the default message “BYE” in annex A.2.8 applying condition A3 or A4 as appropriate.

200 OK for BYE (Step 11)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 applying condition A5 and A11 (in addition to any other applicable conditions).

12.13c MT MTSI speech call Successful with preconditions at originating UE and without preconditions at terminating UE

12.13c.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated speech call setup when using IMS Multimedia Telephony without preconditions after received INVITE request includes the "precondition" option-tag in the Supported header field. This process is described in 3GPP TS 24.229 [10], clauses 5.1.4 and 6.2, TS 24.173 [65] and TS 26.114 [66].

12.13c.2 Conformance requirement

same as 12.13 except

[TS 24.229, Rel-14, clause 5.1.4.1]:

During the session initiation, if local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

…

b) the received INVITE request includes the "precondition" option-tag in the Supported header field, and the precondition mechanism is disabled as specified in subclause 5.1.5A, the terminating UE shall not use the precondition mechanism:

Reference(s)

3GPP TS 24.229 [10] clause 5.1.4.1.

12.13c.3 Test purpose

1) To verify that, when initiating MT MTSI speech call the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SDP contents for negotiating media without preconditions after received INVITE request includes the "precondition" option-tag in the Supported header field.

12.13c.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipp5ed into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-6			Steps 1-6 defined in annex C.11	MTSI MT speech call. Referred from 36.508 [94] table 4.5A.7.3-1 for a UE with E-UTRA support.
7			Step 9 defined in annex C.11	The UE responds to INVITE with 180 Ringing
8-9			Step 12-13 defined in annex C.11	SS responds to INVITE with a 200 OK final response and SS acknowledges the receipt of 200 OK for INVITE.
10-11			Step 14-15 defined in annex C.11	The SS sends BYE to release the call and UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported option-tag	precondition
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line	
Reason-Phrase	Not checked
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Note 1: At least one "c=" field shall be present. Note 2: The values for fmt, payload type and format are not checked Note 3: Parameters for the AMR codec are not checked

180 Ringing (Step 7)

Use the default message “180 Ringing for INVITE” in annex A.2.6 applying condition A2 (in addition to any other applicable conditions).

BYE (Step 10)

Use the default message “BYE” in annex A.2.8 applying condition A3 or A4 as appropriate.

200 OK for BYE (Step 11)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 applying condition A5 and A11 (in addition to any other applicable conditions).

12.14 Void

12.15 Void

12.16 MO MTSI Text call

12.16.1 Definition

Test to verify that the UE correctly performs mobile originated call setup and release for MTSI text call.

12.16.2 Conformance requirement

[TS 24.229, clause 5.1.3.1]

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;and
- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

[TS 24.229, clause 6.1.2]

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

…

If the desired QoS resources for one or more media streams are available at the UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

The following RTP payload format shall be used:

- T.140 text conversation RTP payload format according to RFC 4103.

Real-time text shall be the only payload type in its RTP stream because the RTP sequence numbers are used for loss detection and recovery. The redundant transmission format shall be used for keeping the effect of packet loss low.

Reference(s)

3GPP TS 24.229 [10] clauses 5.1.3.1, 6.1.2, TS 26.114[66] clause 6.2.5, 7.3.1 and 7.4.4.

12.16.3 Test purpose

1) To verify that when initiating MO MTSI text call the UE performs correct exchange of SIP protocol signalling messages for setting up the session.
2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.
3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.
4) To verify that the UE is able to release the call.

12.16.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

1) Execute annex C.15

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.15	MTSI MO text call

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable.

Specific Message Content

-

12.16.5 Test requirements

The UE shall send requests and responses as described in clause 12.16.4.

12.17 MT MTSI text call

12.17.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated text call setup when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.4.1, TS 24.173 [65] and TS 26.114 [66].

12.17.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

[TS 26.114, clause 7.4.4]

The following RTP payload format shall be used:

- T.140 text conversation RTP payload format according to RFC 4103.

Real-time text shall be the only payload type in its RTP stream because the RTP sequence numbers are used for loss detection and recovery. The redundant transmission format shall be used for keeping the effect of packet loss low.

Reference(s)

3GPP TS 24.229 [10] clauses 5.1.4.1 TS 26.114 [66] clause 6.2.5, 7.3 and1, 7.4.4.

12.17.3 Test purpose

1) To verify that, when initiating MT MTSI text call and SS has resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

12.17.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBAonly) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

1) Execute annex C.13

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-10			Steps defined in annex C.13	MTSI MT text call

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable

Specific Message Content

-

12.17.5 Test requirements

The UE shall send requests and responses as described in clause 12.17.4

12.18 Void

12.18a Void

12.18b Void

12.19 Void

12.19a Void

12.19b Void

12.20 Void

12.20a Void

12.21 MO MTSI Video call

12.21.1 Definition

Test to verify that the UE correctly performs IMS mobile originated video call setup and release when using IMS Multimedia Telephony with preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.21.2 Conformance requirement

[TS 24.229, clause 6.1.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,
- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566, unless the UE knows that the precondition mechanism is supported by the remote UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which:

- the related local preconditions are set to meet, using the segmented status type, as defined in RFC 3312 and RFC 4032; and
- the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec for one or more media streams, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

[TS 26.114 Rel-8, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

In addition they should support:

- ITU-T Recommendation H.263 [22] Profile 3 Level 45;
- MPEG-4 (Part 2) Visual [23] Simple Profile Level 3with the following constraints:
    - Number of Visual Objects supported shall be limited to 1.
    - The maximum frame rate shall be 30 frames per second.
    - The maximum f_code shall be 2.
    - The intra_dc_vlc_threshold shall be 0.
    - The maximum horizontal luminance pixel resolution shall be 352 pels/line.
    - The maximum vertical luminance pixel resolution shall be 288 pels/VOP.
    - If AC prediction is used, the following restriction applies: QP value shall not be changed within a VOP (or within a video packet if video packets are used in a VOP). If AC prediction is not used, there are no restrictions to changing QP value.
- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Baseline Profile Level 1.1 with constraint_set1_flag=1 and without requirements on output timing conformance (annex C of [24]). Each sequence parameter set of H.264 (AVC) shall contain the vui_parameters syntax structure including the num_reorder_frames syntax element set equal to 0.

[TS 26.114 Rel-10, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile (CBP) Level 1.2.

In addition they should support:

    - ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile Level 3.1.

In addition they may support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

[TS 26.114, clause 6.2.1a2]:

For voice and real-time text, SDPCapNeg shall be used when offering AVPF the first time for a new media type in the session since the support for AVPF in the answering client is not known at this stage. For video, an MTSI client shall either offer AVPF and AVP together using SDPCapNeg, or the MTSI client shall offer only AVPF, without using SDPCapNeg. If an MTSI client has offered only AVPF for video, and then receives as response either an SDP answer where the video media component has been rejected, or an SIP 488 or 606 failure response with an SDP body indicating that only AVP is supported for video media, the MTSI client should send a new SDP offer with AVP as transport for video. Subsequent SDP offers, in a re-INVITE or UPDATE, may offer AVPF without SDPCapNeg if it is known from an earlier re-INVITE or UPDATE that the answering client supports this RTP profile. If the offer includes only AVP then SDPCapNeg does not need to be used, which can occur for: text; speech if RTCP is not used; and in re-INVITEs or UPDATEs where the RTP profile has already been negotiated for the session in a preceding INVITE or UPDATE.

When offering AVP and AVPF using SDPCapNeg, the MTSI client shall offer AVP on the media (m=) line and shall offer AVPF using SDPCapNeg mechanisms. The SDPCapNeg mechanisms are used as follows:

- The support for AVPF is indicated in an attribute (a=) line using the transport capability attribute 'tcap'. AVPF shall be preferred over AVP.
- At least one configuration using AVPF shall be listed using the attribute for potential configurations 'pcfg'.

[TS 26.114, clause 6.2.3]:

If video is used in a session, the session setup shall determine the bandwidth, RTP profile, video codec, profile and level. The "imageattr" attribute as specified in [76] should be supported.

An MTSI client shall offer AVPF for all media streams containing video. RTP profile negotiation shall be done as described in clause 6.2.1a.

Examples of SDP offers and answers for video can be found in clause A.4.

NOTE: For H.264 / MPEG-4 (Part 10) AVC, the optional max-rcmd-nalu-size receiver-capability parameter of RFC 3984 [25] should be set to the smaller of the MTU size (if known) minus header size or 1 400 bytes (otherwise).

[TS 26.114, clause 7.3.1]:

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556. Therefore, an MTSIclient shall include the "b=RS:" and "b=RR:" fields in SDP, and shall be able to interpret them. There shall be an upper limit on the allowed RTCP bandwidth for each RTP session signalled by the MTSI client. This limit is defined as follows:

- 4 000 bps for the RS field (at media level);
- 3 000 bps for the RR field (at media level).

Reference(s)

3GPP TS 24.229 [10], clauses 6.1.1 and 6.1.2, and TS 26.114 [66], clauses 5.2.2, 6.2.1a2, 6.2.3 and 7.3.1.

12.21.3 Test purpose

1) To verify that when initiating MO video call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and
2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1).
3) To verify that the UE is able to release the video call.

12.21.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.8.3-1, steps 1 to 15.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.25	MTSI MO video call. Referred from 36.508 [94] table 4.5A.8.3-1 for a UE with E-UTRA support.
14	→		BYE	The UE releases the call with BYE
15	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Steps 1 - 13 as specified in annex C.25

BYE (Step 14)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 15)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

12.21.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 14: the UE shall send a BYE request with the correct content, according to common message definitions

12.22 MT MTSI Video call

12.22.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated video call setup when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.22.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

If local resource reservation is not required by the terminating UE andthe terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header and:

- the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

[TS 24.229, clause 6.1.3]

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, it shall set the media streams to active mode by applying the procedures described in RFC 4566 with respect to setting the direction of media streams.

…

Upon sending a SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

[TS 26.114 Rel-8, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

In addition they should support:

- ITU-T Recommendation H.263 [22] Profile 3 Level 45;

- MPEG-4 (Part 2) Visual [23] Simple Profile Level 3with the following constraints:

  - Number of Visual Objects supported shall be limited to 1.

  - The maximum frame rate shall be 30 frames per second.

  - The maximum f_code shall be 2.

  - The intra_dc_vlc_threshold shall be 0.

  - The maximum horizontal luminance pixel resolution shall be 352 pels/line.

  - The maximum vertical luminance pixel resolution shall be 288 pels/VOP.

  - If AC prediction is used, the following restriction applies: QP value shall not be changed within a VOP (or within a video packet if video packets are used in a VOP). If AC prediction is not used, there are no restrictions to changing QP value.

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Baseline Profile Level 1.1 with constraint_set1_flag=1 and without requirements on output timing conformance (annex C of [24]). Each sequence parameter set of H.264 (AVC) shall contain the vui_parameters syntax structure including the num_reorder_frames syntax element set equal to 0.

[TS 26.114 Rel-10, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile (CBP) Level 1.2.

In addition they should support:

  - ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile Level 3.1.

In addition they may support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

[TS 26.114, clause 6.2.1a3]:

An invited MTSI client should accept using AVPF whenever supported. If AVPF has been offered using SDPCapNeg and is to be used in the session then the MTSI client shall:

- select one configuration out of the potential configurations defined in the SDP offer for using AVPF;
- indicate in the media (m=) line of the SDP answer that the profile to use is AVPF; and
- indicate the selected configuration for using AVPF in the attribute for actual configurations ‘acfg’.

If AVP is to be used then the MTSI shall not indicate any SDPCapNeg attributes for using AVPF in the SDP answer.

[TS 26.114, clause 6.2.3]:

If video is used in a session, the session setup shall determine the bandwidth, RTP profile, video codec, profile and level. The "imageattr" attribute as specified in [76] should be supported.

An MTSI client shall offer AVPF for all media streams containing video. RTP profile negotiation shall be done as described in clause 6.2.1a.

Examples of SDP offers and answers for video can be found in clause A.4.

NOTE: For H.264 / MPEG-4 (Part 10) AVC, the optional max-rcmd-nalu-size receiver-capability parameter of RFC 3984 [25] should be set to the smaller of the MTU size (if known) minus header size or 1 400 bytes (otherwise).

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229 [10] clauses 5.1.4.1, 6.1.3, TS 26.114 [66] clause 5.2.2, 6.2.1a3,6.2.3, 6.2.5 and 7.3.1.

12.22.3 Test purpose

1) To verify that, when initiating MT MTSI video call and SS needs to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.
2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.
3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.
4) To verify that the UE is able to release the call.

12.22.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipp5ed into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-27) UE executes the procedures described in TS 36.508 [94] table 4.5A.9.3-1, steps 1 to 27.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.26	MTSI MT video call. Referred from 36.508 [94] table 4.5A.9.3-1 for a UE with E-UTRA support.

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable

Specific Message Content

None.

12.22.5 Test requirements

The UE shall send requests and responses as described in clause 12.22.4

12.23 MO MTSI speech call / EVS

12.23.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup with EVS when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.23.2 Conformance requirement

[TS 26.114, clause 6.2.2.2]

When speech is offered, an MTSI client in terminal sending a first SDP offer in the initial offer-answer negotiation shall include at least one RTP payload type for AMR-NB and the MTSI client in terminal shall support and offer a configuration, where the MTSI client in terminal includes the parameter settings as defined in Table 6.1.

If wideband speech is also offered, then the SDP offer shall also include at least one RTP payload type for AMR-WB according to RFC4867 [28] and the MTSI client in terminal shall support and offer a configuration, where the MTSI client in terminal includes the parameter settings as defined in Table 6.1.

If super-wideband speech is offered, the SDP offer shall include at least one RTP payload type for EVS and the MTSI client in terminal shall support a configuration where the MTSI client in terminal includes the parameter settings as defined in Table 6.2a.

If full band speech is offered, the SDP offer shall include at least one RTP payload type for EVS and the MTSI client in terminal shall support a configuration where the MTSI client in terminal includes the parameter settings as defined in Table 6.2a.

When EVS is offered, the MTSI client in terminal shall support and offer a configuration, where the MTSI client in terminal includes the parameter settings as defined in Table 6.2a. When EVS is offered, the RTP payload type shall also use parameters for EVS AMR-WB IO mode as defined in Table 6.1, except for the 'ecn-capable-rtp' and 'leap ect' parameters.

NOTE 1: RFC4867 can also be used for EVS AMR-WB IO when EVS is supported.

NOTE 2: ECN-triggered adaptation is currently undefined for EVS. This does not prevent ECN-triggered adaptation from being negotiated and used for AMR or AMR-WB.

Clause 5.2.1.6 describes the preference order for how different configurations should be ordered in the list of payload type numbers that is given on the m= line.

Table 6.1: SDP parameters for AMR-NB or AMR-WB, when the MTSI client in terminal offers the bandwidth-efficient payload format

Parameter	Usage
octet-align	Shall not be included
mode-set	Shall not be included
mode-change-period	Shall not be included
mode-change-capability	Shall be set to 2
mode-change-neighbor	Shall not be included
maxptime	Shall be set to 240, see also Table 7.1
crc	Shall not be included
robust-sorting	Shall not be included
interleaving	Shall not be included
ptime	Shall be set according to Table 7.1
channels	Shall either be set to 1 or be omitted
max-red	Shall be included and shall be set to 220 or less
ecn-capable-rtp: leap ect=0	Shall be included if offering to use ECN and if the session setup allows for bit-rate adaptation

Table 6.2: SDP parameters for AMR-NB or AMR-WB, when the MTSI client in terminal offers the octet-aligned payload format

Parameter	Usage
octet-align	Shall be set to 1
mode-set	Shall not be included
mode-change-period	Shall not be included
mode-change-capability	Shall be set to 2
mode-change-neighbor	Shall not be included
maxptime	Shall be set to 240, see also Table 7.1
crc	Shall not be included
robust-sorting	Shall not be included
interleaving	Shall not be included
ptime	Shall be set according to Table 7.1
channels	Shall either be set to 1 or be omitted
max-red	Shall be included and shall be set to 220 or less
ecn-capable-rtp: leap ect=0	Shall be included if offering to use ECN and if the session setup allows for bit-rate adaptation

Table 6.2a: SDP parameters for EVS Primary mode, when the MTSI client in terminal offers EVS

Parameter	Usage
ptime	Shall be set according to Table 7.1
maxptime	Shall be set to 240, see also Table 7.1
dtx	MTSI client in terminal shall not include dtx in the initial SDP offer.
dtx-recv	MTSI client in terminal shall not include dtx-recv.
hf-only	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
evs-mode-switch	MTSI client in terminal shall not include evs-mode-switch in the initial SDP offer.
br	An MTSI client in terminal supporting the EVS codec is required to support the entire bit-rate range but may offer a smaller bit-rate range or even a single bit-rate.
br-send	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
br-recv	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
bw	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
bw-send	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
bw-recv	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
ch-send	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
ch-recv	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
cmr	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
ch-aw-recv	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
channels	The SDP offer-answer considerations in 3GPP TS 26.445 [125] apply.
max-red	Shall be included and shall be set to 220 or less.

When the channels parameter is omitted then this means that one channel is being offered.

The mode-set parameter is omitted, allowing maximum freedom for the visited network.

The mode-change-capability parameter is included and set to 2, to support potential interworking with 2G radio access (GERAN).

An example of an SDP offer for AMR-NB is shown in Table A.1.1. An example of an SDP offer for both AMR-NB and AMR-WB is shown in Table A.1.2. An example of SDP offer for AMR-NB, AMR-WB, and EVS is shown in Table A.14.1.

An SDP example for offering and accepting a dual-mono session for EVS is shown in Annex A.14.1 and A.14.3.

An MTSI client in terminal may divide the offer-answer negotiation into several phases and offer different configurations in different SDP offers. If this is done then the first SDP offer in the initial offer-answer negotiation shall include the most preferable configurations. For AMR-NB, this means that the first SDP offer in the initial offer-answer negotiation shall include at least one RTP payload type for AMR-NB with the parameters as defined in Table 6.1. If wideband speech is offered then the first SDP offer in the initial offer-answer negotiation shall include also at least one RTP payload type for AMR-WB with the parameters as defined in Table 6.1. This also means that offers for octet-aligned payload format do not need to be included in the first SDP offer. If super-wideband or full band speech is offered, the first SDP offer in the initial offer-answer negotiation shall include at least one RTP payload type for EVS with the parameters as defined in [125]. One example of dividing the offer-answer negotiation into two phases, and the corresponding SDP offers, is shown in clause A.1.1.2.2.

NOTE: Dividing the offer-answer negotiation into several phases may lead to never offering the less preferred configurations, if the other end-point accepts to use at least one of the configurations offered in the initial SDP offer.

If the speech media is re-negotiated during the session then the knowledge from earlier offer-answer negotiations should be used in order to shorten the session re-negotiation time. I.e., failed offer-answer transactions shall not be repeated.

Reference(s)

TS 26.114 [66], clause 6.2.2.2.

12.23.3 Test purpose

1) To verify that when initiating MO MTSI speech call and SS needs to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

12.23.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-14) The UE executes the procedure described in TS 36.508 [94] table 4.5A.19.3-1 steps 1 to 14.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.44	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.19.3-1 for a UE with E-UTRA support.
13A			The UE is triggered by MMI to release the call	
14	→		BYE	The UE releases the call with BYE
15	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

None.

12.23.5 Test requirements

The UE shall send requests and responses as described in clause 12.23.4.

12.24 MT MTSI speech call / EVS

12.24.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated voice call setup with EVS when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.24.2 Conformance requirement

[TS 26.114, clause 6.2.2.3]

An MTSI client in terminal must understand all the payload format options that are defined in RFC 4867 [28], and in [125]. It does not have to support operating according to all these options but must be capable to properly accepting or rejecting all options.

The SDP answer depends on many factors, for example:

- what is included in the SDP offer and in what preference order that is defined. The SDP offer will probably be different if it is generated by another MTSI client in terminal, by an MTSI MGW, a TISPAN client or some other VoIP client that does not follow this specification;
- if terminal and/or network resources are available; and:
- if there are other configurations, for example defined with OMA-DM, that mandate, recommend or prevent some configurations.

Table 6.3 describes requirements and recommendations for handling of the AMR payload format parameters and for how to generate the SDP answer.

NOTE: An MTSI client in terminal may support more features than what is required by this specification, e.g. crc, robust sorting and interleaving. Table 6.3 describes the handling of the AMR payload format parameters when the MTSI client implementation supports only those features that are required by this specification. Tables 6.3a-6.3c describe the handling of the EVS payload format parameters.

Table 6.3: Handling of the AMR-NB and AMR-WB SDP parameters in the received SDP offer and in the SDP answer

Parameter in the received SDP offer	Comments	Handling
Codec	Wide-band speech is preferable over narrow-band speech	If both AMR-WB and AMR-NB are offered and if AMR-WB is supported by the answering MTSI client in terminal then it shall select to use the AMR-WB codec and include this codec in the SDP answer, unless another preference order is indicated in the SDP offer. If the MTSI client in terminal only supports AMR-NB then this codec shall be selected to be used and shall be included in the SDP answer. The SDP answer shall only include one RTP Payload Type for speech, see NOTE 1.
octet-align	Both the bandwidth-efficient and the octet-aligned payload formats are supported by the MTSI client in terminal. MTSI MGWs for GERAN or UTRAN are likely to either not include the octet-align parameter or to offer octet-align=0. The bandwidth-efficient payload format is preferable over the octet-aligned payload format.	The offer shall not be rejected purely based on the offered payload format variant. If both bandwidth-efficient and octet-aligned are included in the received SDP offer then the MTSI client in terminal shall select the bandwidth-efficient payload format and include it in the configuration in the SDP answer.
mode-set	The MTSI client in terminal can interoperate properly with whatever mode-set the other end-point offers or if no mode-set is offered. The possibilities to use the higher bit rate codec modes also depend on the offered bandwidth. MTSI MGWs for GERAN or UTRAN inter-working are likely to include the mode-set in the offer if in case the intention is to use TFO or TrFO. Mode sets that give more adaptation possibilities are preferable over mode-sets with fewer or no adaptation possibilities. An MTSI client in terminal may be configured with a preferred mode set. Otherwise, the preferred mode-set for AMR-NB is {12.2, 7.4, 5.9, 4.75} and for AMR-WB it is {12.65, 8.85 and 6.60}.	The offer shall not be rejected purely based on the offered mode-set. If only one mode-set is offered then the MTSI client in terminal shall select to use this and include the same mode-set in the SDP answer. If several different payload types for the same codec with different mode-sets (possibly including one or more payload type without mode set) are included in the received SDP offer, then the MTSI client in terminal should select in the first hand the mode-set that provides the largest degrees of freedom for codec mode adaptation and in the second hand the mode-set that is closest to the preferred mode sets. If only a payload type without mode-set has been offered, or if an MTSI client in terminal selects a payload type without mode-set from among the offered ones, and the MTSI client in terminal intends to use only some modes (e.g. one of the preferred mode sets defined at left), then the MTSI client in terminal should include these modes as the mode-set. There are also dependencies between the mode-set and the SDP b=AS bandwidth parameter; see Clause 6.2.5.2.
mode-change-period	The MTSI client in terminal can interoperate properly with whatever mode-change-period the other end-point offers. MTSI MGWs for GERAN or UTRAN inter-working are likely to include mode-change-period=2 in the offer if in case the intention is to use TFO or TrFO.	The offer shall not be rejected purely based on the offered mode-change-period. If the received SDP offer defines mode-change-period=2 then this information shall be used to determine the mode changes for AMR-NB or AMR-WB encoded media that the MTSI client in terminal sends. The MTSI client in terminal should not include the mode-change-period parameter in the SDP answer since it has no corresponding limitations.

Parameter in the received SDP offer	Comments	Handling
mode-change-capability	The MTSI client in terminal can interoperate with whatever capabilities the other end-point declares.	The offer shall not be rejected purely based on the offered mode-change-capability. The mode-change-capability information should be used to determine a proper value, or prevent using an improper value, for mode-change-period in the SDP answer, see above. If the offer includes mode-change-capability=1, then the MTSI client in terminal shall not offer mode-change-period=2 in the answer. The MTSI client in terminal shall include mode-change-capability=2 in the SDP answer since it is required to support restricting mode changes to every other frame.
mode-change-neighbour	The MTSI client in terminal can interoperate with whatever limitations the other end-point offers.	The offer shall not be rejected purely based on the offered mode-change-neighbour. The MTSI client in terminal shall use this information to determine how mode changes can be performed for AMR-NB or AMR-WB encoded media that the MTSI client in terminal sends. The MTSI client in terminal shall not include the mode-change-neighbour parameter in the SDP answer since it has no corresponding limitations.
maxptime	The MTSI client in terminal can interoperate with whatever value that is offered. The MTSI client in terminal may also use this information to determine a suitable value for max-red in the SDP answer.	The offer shall not be rejected purely based on the offered maxptime. The MTSI client in terminal shall use this information to control the packetization when sending RTP packets to the other end-point, see also clause 7.4.2. The maxptime parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes both the max-red and ptime parameter then the MTSI client in terminal may choose to use this information to define a suitable value for maxptime in the SDP answer, see NOTE 2. The MTSI client in terminal may also choose to set the maxptime value to 240, regardless of the ptime and/or max-red parameters in the SDP offer. The maxptime value in the SDP answer shall not be smaller than ptime value in the SDP answer. The maxptime value should be selected to give at least some room for adaptation.
crc	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.
robust-sorting	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.
interleaving	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.

Parameter in the received SDP offer	Comments	Handling
ptime	The MTSI client in terminal can interoperate with whatever value that is offered.	The offer shall not be rejected purely based on the offered ptime. The MTSI client in terminal should use this information and should use the requested packetization when sending RTP packets to the other end-point. The MTSI client should use the ptime value to determine how many non-redundant speech frames that can be packed into the RTP packets. The requirements in clause 7.4.2 shall be followed even if ptime in the SDP offer is larger than 80. The ptime parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes the ptime parameters then the MTSI client in terminal may choose to use this information to define a suitable value for ptime in the SDP answer, see NOTE 3. The MTSI client in terminal may also choose to set the ptime value in the SDP answer according to Table 7.1, regardless of the ptime parameter in the SDP offer. The ptime value in the SDP answer shall not be larger than the maxptime value in the SDP answer.
channels	The number of channels may either be explicitly indicated in the SDP by including '/1', '/2', etc. on the a=rtpmap line, but the number of channels may also be omitted. When the number of channels is omitted then the default rule is that one channel is being offered. The MTSI client in terminal is only required to support audio media using one channel. Offered RTP payload types with more than one channel may therefore have to be rejected.	When the MTSI client in terminal accepts an offer for single-channel audio then the SDP answer shall either explicitly indicate '/1' or omit the channels parameter. When the MTSI client in terminal accepts an offer for multi-channel audio then the number of channels shall be included in the SDP answer.
max-red	The MTSI client in terminal may use this information to bound the delay for receiving redundant frames. The MTSI client in terminal may also use this information to determine a suitable value for maxptime in the SDP answer.	The max-red parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes both the ptime and maxptime parameters then the MTSI client in terminal may choose to use this information to define a suitable value for max-red in the SDP answer, see NOTE 2. The MTSI client in terminal may also choose to set the max-red value to 220. The max-red value in the SDP answer should be selected to give at least some room for adaptation.
ecn-capable-rtp: leap ect=0	An MTSI client in terminal uses this SDP attribute to offer ECN for RTP-transported media	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation
NOTE 1: An MTSI client may include both a speech coded, e.g. AMR-NB or AMR-WB, and 'telephone-events' for DTMF in the SDP answer, see 3GPP TS 24.229 Clause 6.1, [7]. NOTE 2: It is possible to use the following relationship between maxptime, ptime and max-red: maxptime = ptime + max-red. There is however no mandatory requirement that these parameters must be aligned in this way. NOTE 3: It may be wise to use the same ptime value in the SDP answer as was given in the SDP offer, especially if the ptime in the SDP offer is larger than 20, since a value larger than the frame length indicates that the other end-point is somehow packet rate limited.		

If an SDP offer is received from another MTSI client in terminal using the AMR-NB or AMR-WB codec, then the SDP offer will include configurations as described in Table 6.1 and Table 6.2. If the MTSI client in terminal chooses to accept the offer for using the AMR-NB or AMR-WB codec, as configured in Table 6.1 or Table 6.2 then the MTSI client in terminal shall support a configuration where the MTSI client in terminal creates an SDP answer containing an RTP payload type for the AMR-NB and AMR-WB codec as shown in Table 6.4.

Table 6.3a: Handling of SDP parameters common to EVS Primary and EVS AMR-WB IO in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
ptime		
maxptime		
dtx		MTSI client in terminal shall not include dtx in the initial SDP offer. MTSI MGW may modify SDP offer to include dtx in order to disable DTX in the session.
dtx-recv		MTSI client in terminal shall not include dtx-recv. MTSI MGW may modify SDP offer or answer in order to disable DTX for the send direction of the receiver of dtx-recv.
hf-only		-
evs-mode-switch	This parameter is used by MTSI MGW either when starting in EVS AMR-WB IO mode instead of EVS Primary mode or when switching between EVS Primary mode and EVS AMR-WB IO mode, e.g., for SRVCC.	MTSI client in terminal shall not include evs-mode-switch in the initial SDP offer. When including evs-mode-switch in the SDP offer during a session, the offeror shall use the requested mode when sending EVS packets. However, if a media stream is already being received, the offeror needs to be prepared to receive packets in both EVS primary and EVS AMR-WB IO modes until receiving the answer. When including evs-mode-switch in the SDP answer during a session, the answerer shall use the requested mode when sending EVS packets. When receiving SDP answer including evs-mode-switch during a session, the offeror shall use the requested mode when sending EVS packets.
max-red	See Table 6.3	
channels	See Table 6.3	

Table 6.3b: Handling of the EVS Primary SDP parameters in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
br		An MTSI client in terminal supporting the EVS codec is required to support the entire bit-rate range but may offer a smaller bit-rate range or even a single bit-rate.
br-send		
br-recv		
bw	The session should start with the maximum bandwidth supported by the initial bit-rate up to the maximum negotiated bandwidth. If a range of bandwidth is negotiated, the codec can operate in any bandwidth in the session but the maximum bandwidth in the range should be used after the start of or update of the session. If a single audio bandwidth higher than narrowband is negotiated, the codec operates in the negotiated bandwidth but can use lower bandwidth(s) in the session, depending on the input signal.	Both the offeror and the answerer shall send according to the bandwidth parameter in the answer.
bw-send		
bw-recv		
ch-send		
ch-recv		
cmr	In EVS AMR-WB IO mode, CMR to the bit-rates of EVS AMR-WB IO mode and NO_REQ is always enabled.	If cmr=-1 and the session is in the EVS Primary mode, MTSI client in terminal shall not transmit CMR. If cmr=-1 and the session is in the EVS AMR-WB IO, MTSI client in terminal shall restrict CMR to values of EVS AMR-WB-IO bit-rates and NO_REQ in the session. MTSI client in terminal is required to accept CMR even when cmr=-1. MTSI client in terminal is required to accept RTP payload without CMR even when cmr=1.
ch-aw-recv		If a positive (2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, the receiver of the parameter shall send partial redundancy (channel-aware mode) at the start of the session using the value as the offset. If ch-aw-recv=0 is declared or not present for a payload type and the payload type is accepted, the receiver of the parameter shall not send partial redundancy (channel-aware mode) at the start of the session. If ch-aw-recv=-1 is declared for a payload type and the payload type is accepted, the receiver of the parameter shall not send partial redundancy (channel-aware mode) in the session. If not present or a non-negative (0, 2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, partial redundancy (channel-aware mode) can be activated or deactivated during the session based on the expected or estimated channel condition through adaptation signalling, such as CMR (see Annex A.2 of [125]) or RTCP based signalling (see clause 10.2). If not present or a non-negative (0, 2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, the partial redundancy offset value can also be adjusted during the session based on the expected or estimated channel condition through adaptation signalling.

Reference(s)

3GPP TS 26.114 [66] clause 6.2.2.3.

12.24.3 Test purpose

1) To verify that, when initiating MT MTSI speech call and SS needs to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

12.24.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) The UE executes the procedures described in TS 36.508 [94] table 4.5A.20.3-1 steps 1 to 26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.45	MTSI MT speech call. Referred from 36.508 [94] table 4.5A.20.3-1 for a UE with E-UTRA support.

Specific Message Content

None.

12.24.5 Test requirements

The UE shall send requests and responses as described in clause 12.24.4.

12.25 MO MTSI speech call / EVS offered but not supported by remote UE / AMR-WB agreed

12.25.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup with EVS and the call is answered with codec AMR-WB when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.25.2 Conformance requirement

[TS 26.114, clause 6.2.2.3]

An MTSI client in terminal must understand all the payload format options that are defined in RFC 4867 [28], and in [125]. It does not have to support operating according to all these options but must be capable to properly accepting or rejecting all options.

The SDP answer depends on many factors, for example:

- what is included in the SDP offer and in what preference order that is defined. The SDP offer will probably be different if it is generated by another MTSI client in terminal, by an MTSI MGW, a TISPAN client or some other VoIP client that does not follow this specification;
- if terminal and/or network resources are available; and:
- if there are other configurations, for example defined with OMA-DM, that mandate, recommend or prevent some configurations.

Table 6.3 describes requirements and recommendations for handling of the AMR payload format parameters and for how to generate the SDP answer.

NOTE: An MTSI client in terminal may support more features than what is required by this specification, e.g. crc, robust sorting and interleaving. Table 6.3 describes the handling of the AMR payload format parameters when the MTSI client implementation supports only those features that are required by this specification. Tables 6.3a-6.3c describe the handling of the EVS payload format parameters.

Table 6.3: Handling of the AMR-NB and AMR-WB SDP parameters in the received SDP offer and in the SDP answer

Parameter in the received SDP offer	Comments	Handling
Codec	Wide-band speech is preferable over narrow-band speech	If both AMR-WB and AMR-NB are offered and if AMR-WB is supported by the answering MTSI client in terminal then it shall select to use the AMR-WB codec and include this codec in the SDP answer, unless another preference order is indicated in the SDP offer. If the MTSI client in terminal only supports AMR-NB then this codec shall be selected to be used and shall be included in the SDP answer. The SDP answer shall only include one RTP Payload Type for speech, see NOTE 1.
octet-align	Both the bandwidth-efficient and the octet-aligned payload formats are supported by the MTSI client in terminal. MTSI MGWs for GERAN or UTRAN are likely to either not include the octet-align parameter or to offer octet-align=0. The bandwidth-efficient payload format is preferable over the octet-aligned payload format.	The offer shall not be rejected purely based on the offered payload format variant. If both bandwidth-efficient and octet-aligned are included in the received SDP offer then the MTSI client in terminal shall select the bandwidth-efficient payload format and include it in the configuration in the SDP answer.
mode-set	The MTSI client in terminal can interoperate properly with whatever mode-set the other end-point offers or if no mode-set is offered. The possibilities to use the higher bit rate codec modes also depend on the offered bandwidth. MTSI MGWs for GERAN or UTRAN inter-working are likely to include the mode-set in the offer if in case the intention is to use TFO or TrFO. Mode sets that give more adaptation possibilities are preferable over mode-sets with fewer or no adaptation possibilities. An MTSI client in terminal may be configured with a preferred mode set. Otherwise, the preferred mode-set for AMR-NB is {12.2, 7.4, 5.9, 4.75} and for AMR-WB it is {12.65, 8.85 and 6.60}.	The offer shall not be rejected purely based on the offered mode-set. If only one mode-set is offered then the MTSI client in terminal shall select to use this and include the same mode-set in the SDP answer. If several different payload types for the same codec with different mode-sets (possibly including one or more payload type without mode set) are included in the received SDP offer, then the MTSI client in terminal should select in the first hand the mode-set that provides the largest degrees of freedom for codec mode adaptation and in the second hand the mode-set that is closest to the preferred mode sets. If only a payload type without mode-set has been offered, or if an MTSI client in terminal selects a payload type without mode-set from among the offered ones, and the MTSI client in terminal intends to use only some modes (e.g. one of the preferred mode sets defined at left), then the MTSI client in terminal should include these modes as the mode-set. There are also dependencies between the mode-set and the SDP b=AS bandwidth parameter; see Clause 6.2.5.2.
mode-change-period	The MTSI client in terminal can interoperate properly with whatever mode-change-period the other end-point offers. MTSI MGWs for GERAN or UTRAN inter-working are likely to include mode-change-period=2 in the offer if in case the intention is to use TFO or TrFO.	The offer shall not be rejected purely based on the offered mode-change-period. If the received SDP offer defines mode-change-period=2 then this information shall be used to determine the mode changes for AMR-NB or AMR-WB encoded media that the MTSI client in terminal sends. The MTSI client in terminal should not include the mode-change-period parameter in the SDP answer since it has no corresponding limitations.

Parameter in the received SDP offer	Comments	Handling
mode-change-capability	The MTSI client in terminal can interoperate with whatever capabilities the other end-point declares.	The offer shall not be rejected purely based on the offered mode-change-capability. The mode-change-capability information should be used to determine a proper value, or prevent using an improper value, for mode-change-period in the SDP answer, see above. If the offer includes mode-change-capability=1, then the MTSI client in terminal shall not offer mode-change-period=2 in the answer. The MTSI client in terminal shall include mode-change-capability=2 in the SDP answer since it is required to support restricting mode changes to every other frame.
mode-change-neighbor	The MTSI client in terminal can interoperate with whatever limitations the other end-point offers.	The offer shall not be rejected purely based on the offered mode-change-neighbour. The MTSI client in terminal shall use this information to determine how mode changes can be performed for AMR-NB or AMR-WB encoded media that the MTSI client in terminal sends. The MTSI client in terminal shall not include the mode-change-neighbour parameter in the SDP answer since it has no corresponding limitations.
maxptime	The MTSI client in terminal can interoperate with whatever value that is offered. The MTSI client in terminal may also use this information to determine a suitable value for max-red in the SDP answer.	The offer shall not be rejected purely based on the offered maxptime. The MTSI client in terminal shall use this information to control the packetization when sending RTP packets to the other end-point, see also clause 7.4.2. The maxptime parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes both the max-red and ptime parameter then the MTSI client in terminal may choose to use this information to define a suitable value for maxptime in the SDP answer, see NOTE 2. The MTSI client in terminal may also choose to set the maxptime value to 240, regardless of the ptime and/or max-red parameters in the SDP offer. The maxptime value in the SDP answer shall not be smaller than ptime value in the SDP answer. The maxptime value should be selected to give at least some room for adaptation.
crc	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.
robust-sorting	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.
interleaving	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.

Parameter in the received SDP offer	Comments	Handling
ptime	The MTSI client in terminal can interoperate with whatever value that is offered.	The offer shall not be rejected purely based on the offered ptime. The MTSI client in terminal should use this information and should use the requested packetization when sending RTP packets to the other end-point. The MTSI client should use the ptime value to determine how many non-redundant speech frames that can be packed into the RTP packets. The requirements in clause 7.4.2 shall be followed even if ptime in the SDP offer is larger than 80. The ptime parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes the ptime parameters then the MTSI client in terminal may choose to use this information to define a suitable value for ptime in the SDP answer, see NOTE 3. The MTSI client in terminal may also choose to set the ptime value in the SDP answer according to Table 7.1, regardless of the ptime parameter in the SDP offer. The ptime value in the SDP answer shall not be larger than the maxptime value in the SDP answer.
channels	The number of channels may either be explicitly indicated in the SDP by including '/1', '/2', etc. on the a=rtpmap line, but the number of channels may also be omitted. When the number of channels is omitted then the default rule is that one channel is being offered. The MTSI client in terminal is only required to support audio media using one channel. Offered RTP payload types with more than one channel may therefore have to be rejected.	When the MTSI client in terminal accepts an offer for single-channel audio then the SDP answer shall either explicitly indicate '/1' or omit the channels parameter. When the MTSI client in terminal accepts an offer for multi-channel audio then the number of channels shall be included in the SDP answer.
max-red	The MTSI client in terminal may use this information to bound the delay for receiving redundant frames. The MTSI client in terminal may also use this information to determine a suitable value for maxptime in the SDP answer.	The max-red parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes both the ptime and maxptime parameters then the MTSI client in terminal may choose to use this information to define a suitable value for max-red in the SDP answer, see NOTE 2. The MTSI client in terminal may also choose to set the max-red value to 220. The max-red value in the SDP answer should be selected to give at least some room for adaptation.
ecn-capable-rtp: leap ect=0	An MTSI client in terminal uses this SDP attribute to offer ECN for RTP-transported media	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation
NOTE 1: An MTSI client may include both a speech coded, e.g. AMR-NB or AMR-WB, and ‘telephone-events’ for DTMF in the SDP answer, see 3GPP TS 24.229 Clause 6.1, [7]. NOTE 2: It is possible to use the following relationship between maxptime, ptime and max-red: maxptime = ptime + max-red. There is however no mandatory requirement that these parameters must be aligned in this way. NOTE 3: It may be wise to use the same ptime value in the SDP answer as was given in the SDP offer, especially if the ptime in the SDP offer is larger than 20, since a value larger than the frame length indicates that the other end-point is somehow packet rate limited.		

If an SDP offer is received from another MTSI client in terminal using the AMR-NB or AMR-WB codec, then the SDP offer will include configurations as described in Table 6.1 and Table 6.2. If the MTSI client in terminal chooses to accept the offer for using the AMR-NB or AMR-WB codec, as configured in Table 6.1 or Table 6.2 then the MTSI client in terminal shall support a configuration where the MTSI client in terminal creates an SDP answer containing an RTP payload type for the AMR-NB and AMR-WB codec as shown in Table 6.4.

Table 6.3a: Handling of SDP parameters common to EVS Primary and EVS AMR-WB IO in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
ptime		
maxptime		
dtx		MTSI client in terminal shall not include dtx in the initial SDP offer. MTSI MGW may modify SDP offer to include dtx in order to disable DTX in the session.
dtx-recv		MTSI client in terminal shall not include dtx-recv. MTSI MGW may modify SDP offer or answer in order to disable DTX for the send direction of the receiver of dtx-recv.
hf-only		-
evs-mode-switch	This parameter is used by MTSI MGW either when starting in EVS AMR-WB IO mode instead of EVS Primary mode or when switching between EVS Primary mode and EVS AMR-WB IO mode, e.g., for SRVCC.	MTSI client in terminal shall not include evs-mode-switch in the initial SDP offer. When including evs-mode-switch in the SDP offer during a session, the offeror shall use the requested mode when sending EVS packets. However, if a media stream is already being received, the offeror needs to be prepared to receive packets in both EVS primary and EVS AMR-WB IO modes until receiving the answer. When including evs-mode-switch in the SDP answer during a session, the answerer shall use the requested mode when sending EVS packets. When receiving SDP answer including evs-mode-switch during a session, the offeror shall use the requested mode when sending EVS packets.
max-red	See Table 6.3	
channels	See Table 6.3	

Table 6.3b: Handling of the EVS Primary SDP parameters in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
br		An MTSI client in terminal supporting the EVS codec is required to support the entire bit-rate range but may offer a smaller bit-rate range or even a single bit-rate.
br-send		
br-recv		
bw	The session should start with the maximum bandwidth supported by the initial bit-rate up to the maximum negotiated bandwidth. If a range of bandwidth is negotiated, the codec can operate in any bandwidth in the session but the maximum bandwidth in the range should be used after the start of or update of the session. If a single audio bandwidth higher than narrowband is negotiated, the codec operates in the negotiated bandwidth but can use lower bandwidth(s) in the session, depending on the input signal.	Both the offeror and the answerer shall send according to the bandwidth parameter in the answer.
bw-send		
bw-recv		
ch-send		
ch-recv		
cmr	In EVS AMR-WB IO mode, CMR to the bit-rates of EVS AMR-WB IO mode and NO_REQ is always enabled.	If cmr=-1 and the session is in the EVS Primary mode, MTSI client in terminal shall not transmit CMR. If cmr=-1 and the session is in the EVS AMR-WB IO, MTSI client in terminal shall restrict CMR to values of EVS AMR-WB-IO bit-rates and NO_REQ in the session. MTSI client in terminal is required to accept CMR even when cmr=-1. MTSI client in terminal is required to accept RTP payload without CMR even when cmr=1.
ch-aw-recv		If a positive (2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, the receiver of the parameter shall send partial redundancy (channel-aware mode) at the start of the session using the value as the offset. If ch-aw-recv=0 is declared or not present for a payload type and the payload type is accepted, the receiver of the parameter shall not send partial redundancy (channel-aware mode) at the start of the session. If ch-aw-recv=-1 is declared for a payload type and the payload type is accepted, the receiver of the parameter shall not send partial redundancy (channel-aware mode) in the session. If not present or a non-negative (0, 2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, partial redundancy (channel-aware mode) can be activated or deactivated during the session based on the expected or estimated channel condition through adaptation signalling, such as CMR (see Annex A.2 of [125]) or RTCP based signalling (see clause 10.2). If not present or a non-negative (0, 2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, the partial redundancy offset value can also be adjusted during the session based on the expected or estimated channel condition through adaptation signalling.

Table 6.3c: SDP parameters for the EVS AMR-WB IO parameters in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
mode-set	See Table 6.3	
mode-change-period		
mode-change-neighbor		
mode-change-capability	The default value is re-defined in comparison to that in [28].	As the default and the only allowed value of mode-change-capability is 2 in EVS AMR-WB IO, it is not required to include this parameter in the SDP offer or answer.

NOTE: ECN-triggered adaptation is currently undefined for EVS. This does not prevent ECN-triggered adaptation from being negotiated and used for AMR or AMR-WB.

Table 6.4: SDP parameters for AMR-NB or AMR-WB for SDP answer when the SDP offer is received from another MTSI client in terminal

Parameter	Usage
octet-align	Shall not be included
mode-set	See Table 6.3
mode-change-period	Shall not be included
mode-change-capability	May be included. If it is included then it shall be set to 2
mode-change-neighbor	Shall not be included
maxptime	Shall be set to 240, see also Table 7.1
crc	Shall not be included
robust-sorting	Shall not be included
interleaving	Shall not be included
ptime	Shall be set according to Table 7.1
channels	Shall either be set to 1 or be omitted
max-red	Shall be included and shall be set to 220 or less
ecn-capable-rtp: leap ect=0	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation

If an SDP offer is received from a MTSI MGW inter-working with CS GERAN/UTRAN, and when the MTSI MGW supports ECN (see also Clause 12.3.3), then it is likely to be configured as shown in Table 6.5 if the MTSI MGW does not support redundancy.

Table 6.5: Expected configuration of SDP parameters for AMR-NB or AMR-WB in an SDP offer from an MTSI MGW inter-working with CS GERAN/UTRAN

Parameter	Usage
octet-align	Either not included or set to 0
mode-set	Included and indicates the codec modes that are allowed in the CS network
mode-change-period	Set to 2
mode-change-capability	Set to 2
mode-change-neighbor	Set to 1 if the CS network is GERAN
maxptime	Set to 80, see also Table 12.1
crc	Not included
robust-sorting	Not included
interleaving	Not included
ptime	Set according to Table 12.1
channels	Set to 1 or parameter is omitted
max-red	Set to 0
ecn-capable-rtp: leap ect=0	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation

If the MTSI client in terminal accepts the offer included in Table 6.5 then the MTSI client in terminal shall support a configuration where the MTSI client in terminal creates an SDP answer containing an RTP payload type for the AMR-NB and AMR-WB codecs as shown in Table 6.6.

Table 6.6: SDP parameters for AMR-NB or AMR-WB for SDP answer when the SDP offer is received from another MTSI MGW

Parameter	Usage
octet-align	Shall be set according to the offer
mode-set	See Table 6.3
mode-change-period	Shall not be included
mode-change-capability	May be included. If it is included then it shall be set to 2
mode-change-neighbor	Shall not be included
maxptime	Shall be set to 240, see also Table 7.1
crc	Shall not be included
robust-sorting	Shall not be included
interleaving	Shall not be included
ptime	Shall be set according to Table 7.1
channels	Shall be set according to the offer
max-red	Shall be included and shall be set to 220 or less
ecn-capable-rtp: leap ect=0	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation

Reference(s)

TS 26.114 [66], clause 6.2.2.3.

12.25.3 Test purpose

1) To verify that when initiating MO MTSI speech call and SS needs to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to answer the call using the codec AMR-WB.

5) To verify that the UE is able to release the call.

12.25.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-14) The UE executes the procedure described in TS 36.508 [94] table 4.5A.19.3-1 steps 1 to 14.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-3			Steps defined in annex C.44	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.19.3-1 for a UE with E-UTRA support.
4	←		183 Session Progress	SS sends an SDP answer.
5	→		PRACK	UE acknowledges and optionally offers a second SDP if a dedicated EPS bearer is established by the network.
6-13			Steps defined in annex C.44	
14			The UE is triggered by MMI to release the	
15	→		BYE	The UE releases the call with BYE
16	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:38* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:3*8 - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* - *a=inactive* [Note 7] Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 1] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 3] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2. Note 6: Void. Note 7: The attribute a=inactive shall be present if it was included in step 2.

PRACK (Step 5)

Use the default message “PRACK” in annex A.2.4 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] [Note 5] - *a=fmtp:* (format) [Note 3, 4] - *a= sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one. Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the AMR codec are not checked Note 5: The AMR channel number shall be "/1" or omitted.

12.25.5 Test requirements

The UE shall send requests and responses as described in clause 12.25.4.

12.25a MT MTSI speech call / EVS offered but not supported by UE / AMR-WB agreed

12.25a.1 Definition

Test to verify that the MT UE not supporting EVS correctly performs IMS voice call establishment with AMR-WB when the call is offered with codec EVS and AMR-WB. This process is described in TS 26.114 [66], clause 6.2.2.3.

12.25a.2 Conformance requirement

[TS 26.114, clause 6.2.2.3]

An MTSI client in terminal must understand all the payload format options that are defined in RFC 4867 [28], and in [125]. It does not have to support operating according to all these options but must be capable to properly accepting or rejecting all options.

The SDP answer depends on many factors, for example:

- what is included in the SDP offer and in what preference order that is defined. The SDP offer will probably be different if it is generated by another MTSI client in terminal, by an MTSI MGW, a TISPAN client or some other VoIP client that does not follow this specification;

- if terminal and/or network resources are available; and:

- if there are other configurations, for example defined with OMA-DM, that mandate, recommend or prevent some configurations.

Table 6.3 describes requirements and recommendations for handling of the AMR payload format parameters and for how to generate the SDP answer.

NOTE: An MTSI client in terminal may support more features than what is required by this specification, e.g. crc, robust sorting and interleaving. Table 6.3 describes the handling of the AMR payload format parameters when the MTSI client implementation supports only those features that are required by this specification. Tables 6.3a-6.3c describe the handling of the EVS payload format parameters.

Table 6.3: Handling of the AMR-NB and AMR-WB SDP parameters in the received SDP offer and in the SDP answer

Parameter in the received SDP offer	Comments	Handling
Codec	Wide-band speech is preferable over narrow-band speech	If both AMR-WB and AMR-NB are offered and if AMR-WB is supported by the answering MTSI client in terminal then it shall select to use the AMR-WB codec and include this codec in the SDP answer, unless another preference order is indicated in the SDP offer. If the MTSI client in terminal only supports AMR-NB then this codec shall be selected to be used and shall be included in the SDP answer. The SDP answer shall only include one RTP Payload Type for speech, see NOTE 1.
octet-align	Both the bandwidth-efficient and the octet-aligned payload formats are supported by the MTSI client in terminal. MTSI MGWs for GERAN or UTRAN are likely to either not include the octet-align parameter or to offer octet-align=0. The bandwidth-efficient payload format is preferable over the octet-aligned payload format.	The offer shall not be rejected purely based on the offered payload format variant. If both bandwidth-efficient and octet-aligned are included in the received SDP offer then the MTSI client in terminal shall select the bandwidth-efficient payload format and include it in the configuration in the SDP answer.
mode-set	The MTSI client in terminal can interoperate properly with whatever mode-set the other end-point offers or if no mode-set is offered. The possibilities to use the higher bit rate codec modes also depend on the offered bandwidth. MTSI MGWs for GERAN or UTRAN inter-working are likely to include the mode-set in the offer if in case the intention is to use TFO or TrFO. Mode sets that give more adaptation possibilities are preferable over mode-sets with fewer or no adaptation possibilities. An MTSI client in terminal may be configured with a preferred mode set. Otherwise, the preferred mode-set for AMR-NB is {12.2, 7.4, 5.9, 4.75} and for AMR-WB it is {12.65, 8.85 and 6.60}.	The offer shall not be rejected purely based on the offered mode-set. If only one mode-set is offered then the MTSI client in terminal shall select to use this and include the same mode-set in the SDP answer. If several different payload types for the same codec with different mode-sets (possibly including one or more payload type without mode set) are included in the received SDP offer, then the MTSI client in terminal should select in the first hand the mode-set that provides the largest degrees of freedom for codec mode adaptation and in the second hand the mode-set that is closest to the preferred mode sets. If only a payload type without mode-set has been offered, or if an MTSI client in terminal selects a payload type without mode-set from among the offered ones, and the MTSI client in terminal intends to use only some modes (e.g. one of the preferred mode sets defined at left), then the MTSI client in terminal should include these modes as the mode-set. There are also dependencies between the mode-set and the SDP b=AS bandwidth parameter; see Clause 6.2.5.2.
mode-change-period	The MTSI client in terminal can interoperate properly with whatever mode-change-period the other end-point offers. MTSI MGWs for GERAN or UTRAN inter-working are likely to include mode-change-period=2 in the offer if in case the intention is to use TFO or TrFO.	The offer shall not be rejected purely based on the offered mode-change-period. If the received SDP offer defines mode-change-period=2 then this information shall be used to determine the mode changes for AMR-NB or AMR-WB encoded media that the MTSI client in terminal sends. The MTSI client in terminal should not include the mode-change-period parameter in the SDP answer since it has no corresponding limitations.

Parameter in the received SDP offer	Comments	Handling
mode-change-capability	The MTSI client in terminal can interoperate with whatever capabilities the other end-point declares.	The offer shall not be rejected purely based on the offered mode-change-capability. The mode-change-capability information should be used to determine a proper value, or prevent using an improper value, for mode-change-period in the SDP answer, see above. If the offer includes mode-change-capability=1, then the MTSI client in terminal shall not offer mode-change-period=2 in the answer. The MTSI client in terminal shall include mode-change-capability=2 in the SDP answer since it is required to support restricting mode changes to every other frame.
mode-change-neighbor	The MTSI client in terminal can interoperate with whatever limitations the other end-point offers.	The offer shall not be rejected purely based on the offered mode-change-neighbor. The MTSI client in terminal shall use this information to determine how mode changes can be performed for AMR-NB or AMR-WB encoded media that the MTSI client in terminal sends. The MTSI client in terminal shall not include the mode-change-neighbor parameter in the SDP answer since it has no corresponding limitations.
maxptime	The MTSI client in terminal can interoperate with whatever value that is offered. The MTSI client in terminal may also use this information to determine a suitable value for max-red in the SDP answer.	The offer shall not be rejected purely based on the offered maxptime. The MTSI client in terminal shall use this information to control the packetization when sending RTP packets to the other end-point, see also clause 7.4.2. The maxptime parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes both the max-red and ptime parameter then the MTSI client in terminal may choose to use this information to define a suitable value for maxptime in the SDP answer, see NOTE 2. The MTSI client in terminal may also choose to set the maxptime value to 240, regardless of the ptime and/or max-red parameters in the SDP offer. The maxptime value in the SDP answer shall not be smaller than ptime value in the SDP answer. The maxptime value should be selected to give at least some room for adaptation.
crc	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.
robust-sorting	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.
interleaving	The MTSI client in terminal is not required to support this option.	The MTSI client in terminal may have to reject offered RTP payload types including this option.

Parameter in the received SDP offer	Comments	Handling
ptime	The MTSI client in terminal can interoperate with whatever value that is offered.	The offer shall not be rejected purely based on the offered ptime. The MTSI client in terminal should use this information and should use the requested packetization when sending RTP packets to the other end-point. The MTSI client should use the ptime value to determine how many non-redundant speech frames that can be packed into the RTP packets. The requirements in clause 7.4.2 shall be followed even if ptime in the SDP offer is larger than 80. The ptime parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes the ptime parameters then the MTSI client in terminal may choose to use this information to define a suitable value for ptime in the SDP answer, see NOTE 3. The MTSI client in terminal may also choose to set the ptime value in the SDP answer according to Table 7.1, regardless of the ptime parameter in the SDP offer. The ptime value in the SDP answer shall not be larger than the maxptime value in the SDP answer.
channels	The number of channels may either be explicitly indicated in the SDP by including '/1', '/2', etc. on the a=rtpmap line, but the number of channels may also be omitted. When the number of channels is omitted then the default rule is that one channel is being offered. The MTSI client in terminal is only required to support audio media using one channel. Offered RTP payload types with more than one channel may therefore have to be rejected.	When the MTSI client in terminal accepts an offer for single-channel audio then the SDP answer shall either explicitly indicate '/1' or omit the channels parameter. When the MTSI client in terminal accepts an offer for multi-channel audio then the number of channels shall be included in the SDP answer.
max-red	The MTSI client in terminal may use this information to bound the delay for receiving redundant frames. The MTSI client in terminal may also use this information to determine a suitable value for maxptime in the SDP answer.	The max-red parameter shall be included in the SDP answer and shall be an integer multiple of 20. If the received SDP offer includes both the ptime and maxptime parameters then the MTSI client in terminal may choose to use this information to define a suitable value for max-red in the SDP answer, see NOTE 2. The MTSI client in terminal may also choose to set the max-red value to 220. The max-red value in the SDP answer should be selected to give at least some room for adaptation.
ecn-capable-rtp: leap ect=0	An MTSI client in terminal uses this SDP attribute to offer ECN for RTP-transported media	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation
NOTE 1: An MTSI client may include both a speech coded, e.g. AMR-NB or AMR-WB, and 'telephone-events' for DTMF in the SDP answer, see 3GPP TS 24.229 Clause 6.1, [7]. NOTE 2: It is possible to use the following relationship between maxptime, ptime and max-red: maxptime = ptime + max-red. There is however no mandatory requirement that these parameters must be aligned in this way. NOTE 3: It may be wise to use the same ptime value in the SDP answer as was given in the SDP offer, especially if the ptime in the SDP offer is larger than 20, since a value larger than the frame length indicates that the other end-point is somehow packet rate limited.		

If an SDP offer is received from another MTSI client in terminal using the AMR-NB or AMR-WB codec, then the SDP offer will include configurations as described in Table 6.1 and Table 6.2. If the MTSI client in terminal chooses to accept the offer for using the AMR-NB or AMR-WB codec, as configured in Table 6.1 or Table 6.2 then the MTSI client in terminal shall support a configuration where the MTSI client in terminal creates an SDP answer containing an RTP payload type for the AMR-NB and AMR-WB codec as shown in Table 6.4.

Table 6.3a: Handling of SDP parameters common to EVS Primary and EVS AMR-WB IO in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
ptime		
maxptime		
dtx		MTSI client in terminal shall not include dtx in the initial SDP offer. MTSI MGW may modify SDP offer to include dtx in order to disable DTX in the session.
dtx-recv		MTSI client in terminal shall not include dtx-recv. MTSI MGW may modify SDP offer or answer in order to disable DTX for the send direction of the receiver of dtx-recv.
hf-only		-
evs-mode-switch	This parameter is used by MTSI MGW either when starting in EVS AMR-WB IO mode instead of EVS Primary mode or when switching between EVS Primary mode and EVS AMR-WB IO mode, e.g., for SRVCC.	MTSI client in terminal shall not include evs-mode-switch in the initial SDP offer. When including evs-mode-switch in the SDP offer during a session, the offeror shall use the requested mode when sending EVS packets. However, if a media stream is already being received, the offeror needs to be prepared to receive packets in both EVS primary and EVS AMR-WB IO modes until receiving the answer. When including evs-mode-switch in the SDP answer during a session, the answerer shall use the requested mode when sending EVS packets. When receiving SDP answer including evs-mode-switch during a session, the offeror shall use the requested mode when sending EVS packets.
max-red	See Table 6.3	
channels	See Table 6.3	

Table 6.3b: Handling of the EVS Primary SDP parameters in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
br		An MTSI client in terminal supporting the EVS codec is required to support the entire bit-rate range but may offer a smaller bit-rate range or even a single bit-rate.
br-send		
br-recv		
bw	The session should start with the maximum bandwidth supported by the initial bit-rate up to the maximum negotiated bandwidth. If a range of bandwidth is negotiated, the codec can operate in any bandwidth in the session but the maximum bandwidth in the range should be used after the start of or update of the session. If a single audio bandwidth higher than narrowband is negotiated, the codec operates in the negotiated bandwidth but can use lower bandwidth(s) in the session, depending on the input signal.	Both the offeror and the answerer shall send according to the bandwidth parameter in the answer.
bw-send		
bw-recv		
ch-send		
ch-recv		
cmr	In EVS AMR-WB IO mode, CMR to the bit-rates of EVS AMR-WB IO mode and NO_REQ is always enabled.	If cmr=-1 and the session is in the EVS Primary mode, MTSI client in terminal shall not transmit CMR. If cmr=-1 and the session is in the EVS AMR-WB IO, MTSI client in terminal shall restrict CMR to values of EVS AMR-WB-IO bit-rates and NO_REQ in the session. MTSI client in terminal is required to accept CMR even when cmr=-1. MTSI client in terminal is required to accept RTP payload without CMR even when cmr=1.
ch-aw-recv		If a positive (2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, the receiver of the parameter shall send partial redundancy (channel-aware mode) at the start of the session using the value as the offset. If ch-aw-recv=0 is declared or not present for a payload type and the payload type is accepted, the receiver of the parameter shall not send partial redundancy (channel-aware mode) at the start of the session. If ch-aw-recv=-1 is declared for a payload type and the payload type is accepted, the receiver of the parameter shall not send partial redundancy (channel-aware mode) in the session. If not present or a non-negative (0, 2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, partial redundancy (channel-aware mode) can be activated or deactivated during the session based on the expected or estimated channel condition through adaptation signalling, such as CMR (see Annex A.2 of [125]) or RTCP based signalling (see clause 10.2). If not present or a non-negative (0, 2, 3, 5, or 7) value of ch-aw-recv is declared for a payload type and the payload type is accepted, the partial redundancy offset value can also be adjusted during the session based on the expected or estimated channel condition through adaptation signalling.

Table 6.3c: SDP parameters for the EVS AMR-WB IO parameters in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
mode-set	See Table 6.3	
mode-change-period		
mode-change-neighbor		
mode-change-capability	The default value is re-defined in comparison to that in [28].	As the default and the only allowed value of mode-change-capability is 2 in EVS AMR-WB IO, it is not required to include this parameter in the SDP offer or answer.

NOTE: ECN-triggered adaptation is currently undefined for EVS. This does not prevent ECN-triggered adaptation from being negotiated and used for AMR or AMR-WB.

Table 6.4: SDP parameters for AMR-NB or AMR-WB for SDP answer when the SDP offer is received from another MTSI client in terminal

Parameter	Usage
octet-align	Shall not be included
mode-set	See Table 6.3
mode-change-period	Shall not be included
mode-change-capability	May be included. If it is included then it shall be set to 2
mode-change-neighbor	Shall not be included
maxptime	Shall be set to 240, see also Table 7.1
crc	Shall not be included
robust-sorting	Shall not be included
interleaving	Shall not be included
ptime	Shall be set according to Table 7.1
channels	Shall either be set to 1 or be omitted
max-red	Shall be included and shall be set to 220 or less
ecn-capable-rtp: leap ect=0	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation

If an SDP offer is received from a MTSI MGW inter-working with CS GERAN/UTRAN, and when the MTSI MGW supports ECN (see also Clause 12.3.3), then it is likely to be configured as shown in Table 6.5 if the MTSI MGW does not support redundancy.

Table 6.5: Expected configuration of SDP parameters for AMR-NB or AMR-WB in an SDP offer from an MTSI MGW inter-working with CS GERAN/UTRAN

Parameter	Usage
octet-align	Either not included or set to 0
mode-set	Included and indicates the codec modes that are allowed in the CS network
mode-change-period	Set to 2
mode-change-capability	Set to 2
mode-change-neighbor	Set to 1 if the CS network is GERAN
maxptime	Set to 80, see also Table 12.1
crc	Not included
robust-sorting	Not included
interleaving	Not included
ptime	Set according to Table 12.1
channels	Set to 1 or parameter is omitted
max-red	Set to 0
ecn-capable-rtp: leap ect=0	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation

If the MTSI client in terminal accepts the offer included in Table 6.5 then the MTSI client in terminal shall support a configuration where the MTSI client in terminal creates an SDP answer containing an RTP payload type for the AMR-NB and AMR-WB codecs as shown in Table 6.6.

Table 6.6: SDP parameters for AMR-NB or AMR-WB for SDP answer when the SDP offer is received from another MTSI MGW

Parameter	Usage
octet-align	Shall be set according to the offer
mode-set	See Table 6.3
mode-change-period	Shall not be included
mode-change-capability	May be included. If it is included then it shall be set to 2
mode-change-neighbor	Shall not be included
maxptime	Shall be set to 240, see also Table 7.1
crc	Shall not be included
robust-sorting	Shall not be included
interleaving	Shall not be included
ptime	Shall be set according to Table 7.1
channels	Shall be set according to the offer
max-red	Shall be included and shall be set to 220 or less
ecn-capable-rtp: leap ect=0	Shall be included in the SDP answer if accepting an offer to use ECN and if the session setup allows for bit-rate adaptation

Reference(s)

TS 26.114 [66], clause 6.2.2.3.

12.25a.3 Test purpose

1) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

2) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

3) To verify that the UE is able to answer the call using the codec AMR-WB when the UE receives SDP offer including codec EVS and AMR-WB.

12.25a.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Step 1 defined in annex C.45	
2-15			Steps 2-15 defined in annex C.11	

Specific Message Contents

None.

12.26 MT MTSI speech call / EVS / AMR-WB IO mode

12.26.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup with EVS when using IMS Multimedia Telephony. Then a mobile terminated switch from EVS primary mode to EVS AMR-WB IO mode. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

12.26.2 Conformance requirement

[TS 26.114, clause 6.2.2.3]

An MTSI client in terminal must understand all the payload format options that are defined in RFC 4867 [28], and in [125]. It does not have to support operating according to all these options but must be capable to properly accepting or rejecting all options.

The SDP answer depends on many factors, for example:

- what is included in the SDP offer and in what preference order that is defined. The SDP offer will probably be different if it is generated by another MTSI client in terminal, by an MTSI MGW, a TISPAN client or some other VoIP client that does not follow this specification;

- if terminal and/or network resources are available; and:

- if there are other configurations, for example defined with OMA-DM, that mandate, recommend or prevent some configurations.

Table 6.3 describes requirements and recommendations for handling of the AMR payload format parameters and for how to generate the SDP answer.

NOTE: An MTSI client in terminal may support more features than what is required by this specification, e.g. crc, robust sorting and interleaving. Table 6.3 describes the handling of the AMR payload format parameters when the MTSI client implementation supports only those features that are required by this specification. Tables 6.3a-6.3c describe the handling of the EVS payload format parameters.

…

Table 6.3a: Handling of SDP parameters common to EVS Primary and EVS AMR-WB IO in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
ptime		
maxptime		
dtx		MTSI client in terminal shall not include dtx in the initial SDP offer. MTSI MGW may modify SDP offer to include dtx in order to disable DTX in the session.
dtx-recv		MTSI client in terminal shall not include dtx-recv. MTSI MGW may modify SDP offer or answer in order to disable DTX for the send direction of the receiver of dtx-recv.
hf-only		-
evs-mode-switch	This parameter is used by MTSI MGW either when starting in EVS AMR-WB IO mode instead of EVS Primary mode or when switching between EVS Primary mode and EVS AMR-WB IO mode, e.g., for SRVCC.	MTSI client in terminal shall not include evs-mode-switch in the initial SDP offer. When including evs-mode-switch in the SDP offer during a session, the offeror shall use the requested mode when sending EVS packets. However, if a media stream is already being received, the offeror needs to be prepared to receive packets in both EVS primary and EVS AMR-WB IO modes until receiving the answer. When including evs-mode-switch in the SDP answer during a session, the answerer shall use the requested mode when sending EVS packets. When receiving SDP answer including evs-mode-switch during a session, the offeror shall use the requested mode when sending EVS packets.
max-red	See Table 6.3	
channels	See Table 6.3	

…

Table 6.3c: SDP parameters for the EVS AMR-WB IO parameters in the received SDP offer and in the SDP answer

Parameter	Comments	Handling
mode-set	See Table 6.3	
mode-change-period		
mode-change-neighbor		
mode-change-capability	The default value is re-defined in comparison to that in [28].	As the default and the only allowed value of mode-change-capability is 2 in EVS AMR-WB IO, it is not required to include this parameter in the SDP offer or answer.

NOTE: ECN-triggered adaptation is currently undefined for EVS. This does not prevent ECN-triggered adaptation from being negotiated and used for AMR or AMR-WB.

[TS 26.114, clause 12.3.4.]

An MTSI client in terminal (hereinafter “local client”) using 3GPP PS access may be handed over to CS access. By that SRVCC procedure, the end-point of the IP connection moves from the local client to a CS MGW in the CS network, as described in TS 23.216 (SRVCC) [133].

In order to achieve this handover, the MSC server, controlling the CS MGW, sends a SIP INVITE message:

- either to the remote client (in case of SRVCC handover without SRVCC enhancement);
- or to the ATCF (in case of SRVCC handover with ATCF enhancement),

to change the communication end from the MTSI client in terminal to the CS MGW as described in TS 23.237 [134].

If EVS is used between local and remote client before SRVCC and if AMR-WB is used after SRVCC by the local CS UE, an MTSI MGW (e.g. MSC/CS-MGW or ATCF/ATGW) can send the RTCP_APP_EP2I request message, (see clause 10.1.2.10), or a CMR in the RTP payload requesting an EVS AMR-WB IO mode, to the remote client to request that it switches from the EVS Primary mode to the EVS AMR-WB IO mode. The mode-set used in CS shall be included in the RTCP_APP_EP2I request message. Furthermore, the RTCP_APP_EP2I request message also supports signalling to restrict the timing and destination of codec mode changes. An SDP offer/answer negotiation between the MTSI MGW and the remote client can also be performed to align the mode-sets and to optimize the resource usage and also to request switching to the EVS AMR-WB IO mode.

Correspondingly, the RTCP_APP_EI2P request message can be used to switch from the EVS AMR-WB IO mode to the EVS Primary mode, e.g. in case an SRVCC handover to a CS access and a switch to the EVS AMR-WB IO mode is followed by a reverse SRVCC to perform handover back to the PS access. An SDP offer/answer negotiation can also be performed to restore the session, e.g. bitrates, bandwidths and other configuration parameters, to what was used before SRVCC.

Reference(s)

TS 26.114 [66], clause 6.2.2.3 and 12.3.4.

12.26.3 Test purpose

1) To verify that when initiating MO MTSI speech call and SS needs to reserve resources; the UE performs correct exchange of SIP protocol signalling messages for setting up the session.
2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.
3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.
4) To verify that the UE is able to answer the call using the codec AMR-WB IO mode.

12.26.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

0-13) The UE executes the procedure described in TS 36.508 [94] table 4.5A.19.3-1 steps 1 to 14.

14) SS sends a re-INVITE request to the UE.

15) SS expects and receives 200 OK for re-INVITE from the UE.

15A) SS acknowledges the receipt of 200 OK for re-INVITE.

16-19) SS executes the procedure C.33.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.44	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.19.3-1 for a UE with E-UTRA support.
14	←		INVITE	The SS sends re-INVITE with second SDP offer to switch to EVS AMR-WB IO mode.
14A	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
15	→		200 OK	The UE responds to the re-INVITE with a 200 OK final response.
15A	←		ACK	The SS acknowledges the receipt of 200 OK for re-INVITE.
16-19			Steps defined in annex C.33	The SS releases the call.

Specific Message Contents

INVITE (Step 14)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported	
option-tag	*precondition*
Message-body	SDP body copied from the previous 200 OK (C.44 step 6 or 8), and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. - "a=fmtp" line identical to previous SDP sent by SS except that "evs-mode-switch=1" is added.

200 OK (Step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 4] - *s*=(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *EVS/16000* [Note 2] - *a=fmtp:*(format) *evs-mode-switch=1;* [Note 2, 3] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The values for fmt, payload type and format are not checked. Note 3: The evs-mode-switch is checked, but no other codec parameters. Note 4: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

12.26.5 Test requirements

The UE shall send requests and responses as described in clause 12.26.4.

12.27 MO MTSI speech call / SRVCC on MT side / Codec Change from AMR-WB to AMR-NB

12.27.1 Definition

Test to verify that the MO UE correctly performs codec change from AMR-WB to AMR-NB when SRVCC happens on MT UE. This process is described in 3GPP TS 23.237 [155], clauses B.2.1.

12.27.2 Conformance requirement

[TS 23.237, clause B.2.1]:

After SRVCC has been successfully performed (see clauses 6.3.2.1.9.1 and 6.3.2.1.9.2), MSC Sever may initiates a SIP REINVITE to modify the Selected Codec towards the remote end in order to minimize the transcoding points in the voice path.

Figure B.2-1 below illustrates this procedure with the assumption that the remote end supports the selected target RAN codec (B) in the Re-INVITE.

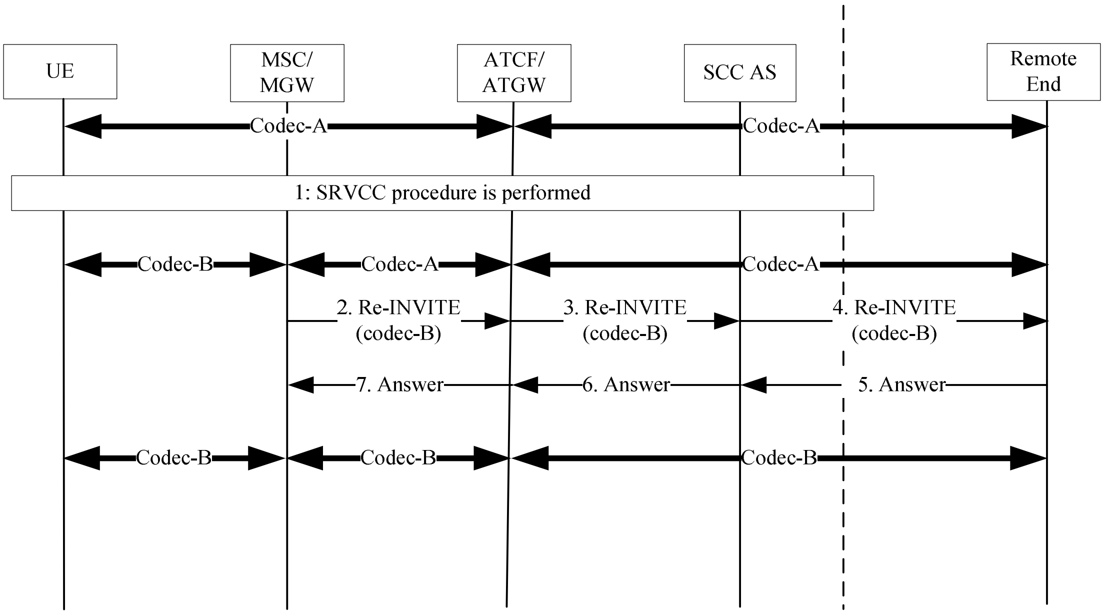

Figure B.2.1-1: Re-negotiation method towards the remote end

1. SRVCC is performed. MSC Server has included all supported codecs into the session transfer request to the ATCF. In this flow the codec list may include the codec that is currently used in the ongoing IMS session and ATCF has selected this codec, therefore there is no transcoding in ATGW but there may be transcoding in CS-MGW. The session between UE and CS-MGW uses the codec-B. The session between CS-MGW, ATGW and remote end uses the codec-A.

NOTE 1: If the codec list from MSC Server does not include the codec that is currently used in the ongoing session, ATCF initiates transcoding.

2. The MSC server sends a Re-INVITE to remote end with list of supported codecs in MSC server to ATCF, codec B is the most preferred codec in the list.

NOTE 2: It may be that the CS MGW or ATGW supports the audio Codec that is compatible or equal to the audio Codec used for the PS session but a change of the codec mode (such as bitrate, audio bandwidth, EVS Primary/AMR-WB IO modes) of the audio Codec used for the PS session is required. In this case the MSC server or ATCF may initiates a signalling towards to remote end to modify the codec mode of the audio Codec used for the PS session. The signalling to modify the codec mode is specific to the audio Codec used for the PS session as discussed in TS 26.114 [35], i.e. this procedure may be taken place by SIP invite, but may also be taken place by RTCP-APP or CMR (Codec Mode Request).

3. ATCF passes the Re-INVITE towards the SCC AS with the codec list.

4. SCC AS performs a remote leg update towards the remote end.

5-7. The remote end accepts the offer and selects the most preferred codec it can support, in this case codec B was selected. From now on the codec B is used e2e in TrFO manner.

Reference(s)

3GPP TS 23.237 [155], clauses B.2.1.

12.27.3 Test purpose

1) To verify that the MO UE correctly performs codec change from AMR-WB to AMR-NB after call establishment.

12.27.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-14) The UE executes the procedure described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14.

15) SS sends a re-INVITE request to the UE.

16) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.

17) SS waits for the UE to respond to the INVITE request with valid 200 OK response..

18) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE..

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.21	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
14	←		INVITE	SS sends re-INVITE with an SDP offer to switch to AMR-NB.
15	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
16	→		200 OK	The UE responds re-INVITE with 200 OK final response.
17	←		ACK	The SS acknowledges the receipt of 200 OK for re-INVITE.

Specific Message Contents

INVITE (Step 14)

Use the default message “INVITE for MT Call” in annex A.2.9 with condition A5 and the following exceptions:

Header/param	Value/remark
Message-body	SDP body copied from the previous 200 OK (C.21 step 6 or 8), and modified as follows: - “o=” line identical to previous SDP sent by SS except that sess-version is incremented. Media description: - *m=audio* (transport port) *RTP/AVP 99 100* - *b=AS:37* - *b=RS:300* - *b=RR:900* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-set=7; octet-align=1 ; max-red=0* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:20* - Attribute for preconditions are removed.

200 OK (Step 16)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 3] - *s*=(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) Note 1: At least one "c=" field shall be present. Note 2: The values for fmt, payload type and format are not checked. Note 3: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

12.27a MO MTSI speech call / SRVCC on MT side / Codec Change from EVS to AMR-NB

12.27a.1 Definition

Test to verify that the MO UE correctly performs codec change from EVS to AMR-NB when SRVCC happens on MT UE. This process is described in 3GPP TS 23.237 [155], clauses B.2.1.

12.27a.2 Conformance requirement

[TS 23.237, clause B.2.1]:

After SRVCC has been successfully performed (see clauses 6.3.2.1.9.1 and 6.3.2.1.9.2), MSC Sever may initiates a SIP REINVITE to modify the Selected Codec towards the remote end in order to minimize the transcoding points in the voice path.

Figure B.2-1 below illustrates this procedure with the assumption that the remote end supports the selected target RAN codec (B) in the Re-INVITE.

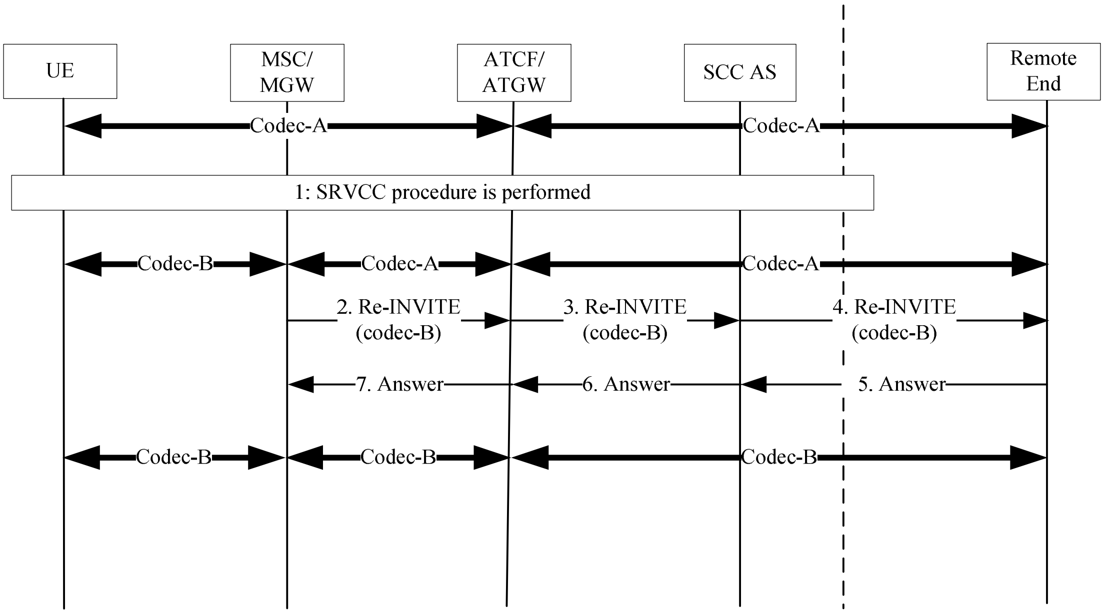

Figure B.2.1-1: Re-negotiation method towards the remote end

1. SRVCC is performed. MSC Server has included all supported codecs into the session transfer request to the ATCF. In this flow the codec list may include the codec that is currently used in the ongoing IMS session and ATCF has selected this codec, therefore there is no transcoding in ATGW but there may be transcoding in CS-MGW. The session between UE and CS-MGW uses the codec-B. The session between CS-MGW, ATGW and remote end uses the codec-A.

NOTE 1: If the codec list from MSC Server does not include the codec that is currently used in the ongoing session, ATCF initiates transcoding.

2. The MSC server sends a Re-INVITE to remote end with list of supported codecs in MSC server to ATCF, codec B is the most preferred codec in the list.

NOTE 2: It may be that the CS MGW or ATGW supports the audio Codec that is compatible or equal to the audio Codec used for the PS session but a change of the codec mode (such as bitrate, audio bandwidth, EVS Primary/AMR-WB IO modes) of the audio Codec used for the PS session is required. In this case the MSC server or ATCF may initiates a signalling towards to remote end to modify the codec mode of the audio Codec used for the PS session. The signalling to modify the codec mode is specific to the audio Codec used for the PS session as discussed in TS 26.114 [35], i.e. this procedure may be taken place by SIP invite, but may also be taken place by RTCP-APP or CMR (Codec Mode Request).

3. ATCF passes the Re-INVITE towards the SCC AS with the codec list.

4. SCC AS performs a remote leg update towards the remote end.

5-7. The remote end accepts the offer and selects the most preferred codec it can support, in this case codec B was selected. From now on the codec B is used e2e in TrFO manner.

Reference(s)

3GPP TS 23.237 [155], clauses B.2.1.

12.27a.3 Test purpose

1) To verify that the MO UE correctly performs codec change from EVS to AMR-NB after call establishment.

12.27a.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-14) The UE executes the procedure described in TS 36.508 [94] table 4.5A.19.3-1 steps 1 to 14.

15) SS sends a re-INVITE request to the UE.

16) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.

17) SS waits for the UE to respond to the INVITE request with valid 200 OK response..

18) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE..

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.44	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.19.3-1 for a UE with E-UTRA support.
14	←		INVITE	SS sends re-INVITE with an SDP offer to switch to AMR-NB.
15	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
16	→		200 OK	The UE responds re-INVITE with 200 OK final response.
17	←		ACK	The SS acknowledges the receipt of 200 OK for re-INVITE.

Specific Message Contents

INVITE (Step 14)

Use the default message "INVITE for MT Call" in annex A.2.9 with condition A5 and the following exceptions:

Header/param	Value/remark
Message-body	SDP body copied from the previous 200 OK (C.44 step 6 or 8), and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Media description: - *m=audio* (transport port) *RTP/AVP 99 100* - *b=AS:37* - *b=RS:300* - *b=RR:900* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-set=7; octet-align=1 ; max-red=0* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:20* - Attribute for preconditions are removed.

200 OK (Step 16)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 3] - *s*=(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) Note 1: At least one "c=" field shall be present. Note 2: The values for fmt, payload type and format are not checked. Note 3: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

12.28 MO MTSI speech call / MO UE cancels call establishment

12.28.1 Definition

Test to verify that the MO UE correctly cancels voice call establishment. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3.

12.28.2 Conformance requirement

[TS 24.229, clause 5.1.3.1]:

If the UE sends a CANCEL request to cancel an initial INVITE request, the UE shall when applicable include in the CANCEL request a Reason header field with a protocol value set to "RELEASE_CAUSE" and a "cause" header field parameter as specified in subclause 7.2A.18.11.2. The UE may also include the "text" header field parameter with reason-text as specified in subclause 7.2A.18.11.2.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.3.

12.28.3 Test purpose

1) To verify that MO UE correctly cancels voice call establishment.

12.28.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-11			Steps 1-11 defined in annex C.21	
11A				The MO UE cancels a voice call establishment manually.
12	→		CANCEL	
13	←		200 OK	SS responds CANCEL with 200 OK.
14	←		487 Request Terminated	SS responds INVITE with 487 Request Terminated
15	→		ACK	UE acknowledges.

Specific Message Contents

Steps 1 - 11 as specified in annex C.21

CANCEL (Step 12)

Use the default message “CANCEL” in annex A.2.15.

487 Request Terminated (Step 14)

Use the default message “487 Request Terminated” in annex A.2.16

ACK (Step 15)

Use the default message “ACK” in annex A.2.7

12.29 MO MTSI Video call / MO UE cancels call establishment

12.29.1 Definition

Test to verify that the MO UE correctly cancels video call establishment. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3.

12.29.2 Conformance requirement

[TS 24.229, clause 5.1.3.1]:

If the UE sends a CANCEL request to cancel an initial INVITE request, the UE shall when applicable include in the CANCEL request a Reason header field with a protocol value set to "RELEASE_CAUSE" and a "cause" header field parameter as specified in subclause 7.2A.18.11.2. The UE may also include the "text" header field parameter with reason-text as specified in subclause 7.2A.18.11.2.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.3.

12.29.3 Test purpose

1) To verify that MO UE correctly cancels video call establishment.

12.29.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-11			Steps 1-11 defined in annex C.25	
11A				The MO UE cancels a video call establishment manually.
12	→		CANCEL	
13	←		200 OK	SS responds CANCEL with 200 OK.
14	←		487 Request Terminated	SS responds INVITE with 487 Request Terminated
15	→		ACK	UE acknowledges.

Specific Message Contents

Steps 1 - 11 as specified in annex C.25

CANCEL (Step 12)

Use the default message "CANCEL" in annex A.2.15.

487 Request Terminated (Step 14)

Use the default message "487 Request Terminated" in annex A.2.16

ACK (Step 15)

Use the default message "ACK" in annex A.2.7

13 Signalling Compression (SIGComp)

13.1 SigComp in the Initial registration

Editor's note: This test case needs to be updated to Release-8.

13.1.1 Definition

Test to verify that the UE can correctly register to IMS services when the P-CSCF supports and uses SigComp. This includes correct decompression by the UE and optional compression by the UE.

13.1.2 Conformance requirement

The UE shall support SigComp as specified in RFC 3320. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486.

…

The UE shall support the SIP dictionary specified in RFC 3485. If compression is enabled, the UE shall use the dictionary to compress the first message.

…

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

…

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

Reference(s)

3GPP TS 24.229 [10], clauses 8.1.1, 8.1.2 and 8.1.3.

13.1.3 Test purpose

1) To verify that the UE performs initial registration, subscription and notification according to 3GPP TS 24.229 [10]. The UE can send messages compressed or not compressed. The UE can announce to support SIP Compression "comp=sigcomp"; and

2) To verify that the UE uses the SIP/SDP dictionary specified in RFC 3485 [25] at least in the first message sent; and

3) To verify that the UE decompresses all the SIP messages sent by the SS in accordance 3GPP TS 24.229 [10] clause 8.1.1. This is tested implicitly by checking the messages sent by the UE verifying the correct exchange of SIP protocol signalling messages.

NOTE: The presence of the SIP Compression announcement “comp=sigcomp” by both UE and P-CSCF indicates the willingness to send or receive SIP messages compressed. The mechanism which controls the willingness to apply SigComp is described in RFC 3486 [26] by sentences containing SHOULD, for this reason the presence of the “comp=sigcomp” parameter from UE side (even if strongly recommended and consistent with the use of compression) is considered optional.

13.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1) IMS registration is initiated on the UE. The SS waits for the UE to send an initial REGISTER request. The SIP Compression announcement “comp=sigcomp” in the Via header and in the Contact header may be included. The message can be sent compressed or not compressed.

2) The SS responds to the initial REGISTER request with a compressed valid 401 Unauthorized response, headers populated according to the 401 response common message definition.

3) The SS waits for the UE to set up a temporary set of security associations and send another REGISTER request over those security associations. The SIP Compression announcement “comp=sigcomp” in the Via header and in the Contact header may be included. The message can be sent compressed or not compressed.

4) The SS responds to the second REGISTER request with a valid compressed 200 OK response, sent over the same temporary set of security associations that the UE used for sending the REGISTER request. The SS shall populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

5) The SS waits for the UE to send a SUBSCRIBE request. The SIP Compression announcement “comp=sigcomp” in the Via and in the Contact header may be included. The message can be sent compressed or not compressed.

6) The SS responds to the SUBSCRIBE request with a valid compressed 200 OK response, headers populated according to the 200 response for SUBSCRIBE common message definition with the SIP Compression announcement “comp=sigcomp” in the record-route header.

7) The SS sends a compressed NOTIFY request for the subscribed registration event package. In the request the Request URI, headers and the request body shall be populated according to the NOTIFY common message definition.

8) The SS waits for the UE to respond to the NOTIFY with a 200 OK response. The message can be sent compressed or not compressed.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The UE sends initial registration for IMS services. with comp=sigcomp in the Via and Contact headers. The message can be sent compressed or not compressed.
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network. This message is sent compressed.
3	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials. The message can be sent compressed or not compressed.
4	←		200 OK	The SS responds with 200 OK. This message is sent compressed.
5	→		SUBSCRIBE	The UE subscribes to its registration event package. The message can be sent compressed or not compressed.
6	←		200 OK	The SS responds with 200 OK. This message is sent compressed.
7	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body. This message is sent compressed.
8	→		200 OK	The UE responds with 200 OK. The message can be sent compressed or not compressed.

Specific Message Contents

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1, condition A1 "Initial unprotected REGISTER". The following exceptions can be used if the UE is willing to receive response and request compressed:

Header/param	Value/remark
Via via-compression	 comp=sigcomp
Contact compression-param	 comp=sigcomp

401 Unauthorized for REGISTER (Step 2)

Use the default message “401 Unauthorized for REGISTER” in annex A.1.2.

REGISTER (Step 3)

Use the default message “REGISTER” in annex A.1.1, condition A2 "Subsequent REGISTER sent over security associations". The following exceptions can be used if the UE is willing to receive response and request compressed:

Header/param	Value/remark
Via via-compression	 comp=sigcomp
Contact compression-param	 comp=sigcomp

200 OK for REGISTER (Step 4)

Use the default message “200 OK for REGISTER” in annex A.1.3.

SUBSCRIBE (Step 5)

Use the default message “SUBSCRIBE for reg-event package” in annex A.1.4. The following exceptions can be used if the UE is willing to receive response and request compressed:

Header/param	Value/remark
Via via-compression	 comp=sigcomp
Contact compression-param	 comp=sigcomp

200 OK for SUBSCRIBE (Step 6)

Use the default message “200 OK for SUBSCRIBE” in annex A.1.5 with the following exceptions:

Header/param	Value/remark
Record-Route compression-param	 comp=sigcomp

NOTIFY (Step 7)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with the following exceptions:

Header/param	Value/remark
Via **via-parm1:** via-compression	 comp=sigcomp

200 OK for NOTIFY (Step 8)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

13.1.5 Test requirements

Step 1: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends initial REGISTER request. If the message has been sent compressed then check the following:

a) the message is sent compressed according to RFC 3320 [24]; and

b) if the message received from the UE is the first compressed message, then the compression shall support SIP dictionary specified in RFC 3485 [25]; and

Step 3: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends second REGISTER request. If the message has been sent compressed then check the following:

a) the message is sent compressed according to RFC 3320 [24]; and

b) if the message received from the UE is the first compressed message, then the compression shall support SIP dictionary specified in RFC 3485 [25]; and

Step 5: SS shall check that, in accordance to the 3GPP TS 24.229 [10] clause 8.1.1, the UE sends a SUBSCRIBE request. If the message has been sent compressed then check the following:

a) the message is sent compressed according to RFC 3320 [24]; and

b) if the message received from the UE is the first compressed message, then the compression shall support SIP dictionary specified in RFC 3485 [25]; and

Step 8: SS shall check that, in accordance to the 3GPP TS 24.229 [10] clause 8.1.1, the UE sends a 200 OK for NOTIFY response. If the message has been sent compressed then check the following:

a) the message is sent compressed according to RFC 3320 [24]; and;

b) if the message received from the UE is the first compressed message, then the compression shall support SIP dictionary specified in RFC 3485 [25].

13.2 SigComp in the MO Call

Editor's note: This test case needs to be updated to Release-8.

13.2.1 Definition

Test to verify that the UE correctly performs IMS mobile originated call setup when the P-CSCF supports and uses SigComp. This includes correct decompression and optional compression by the UE.

13.2.2 Conformance requirement

The UE shall support SigComp as specified in RFC 3320. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486.

…

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

…

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

Reference(s)

3GPPTS 24.229 [10], clauses 8.1.1, 8.1.2, and 8.1.3.

13.2.3 Test purpose

1) To verify that, when initiating MO call, the UE performs the session setup according to 3GPP TS 24.229 [10]. The UE can send messages compressed or not compressed The UE can announce to support SIP Compression "comp=sigcomp"; and

2) To verify that the UE decompresses all the SIP messages sent by the SS in accordance 3GPP TS 24.229 [10] clause 8.1.1. This is tested implicitly by verifying the correct exchange of SIP protocol signalling messages.

NOTE: The presence of the SIP Compression announcement "comp=sigcomp" by both UE and P-CSCF indicates the willingness to send or receive SIP messages compressed. The mechanism which controls the willingness to apply SigComp is described in RFC 3486 [26] by sentences containing SHOULD, for this reason the presence of the "comp=sigcomp" parameter from UE side (even if strongly recommended and consistent with the use of compression) is considered optional.

13.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step (with Compression activated on SS).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

1) MO call is initiated on the UE. SS waits the UE to send an INVITE request with first SDP offer, over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.3. The SIP Compression announcement "comp=sigcomp" in the Via header, in the Route header and in the Contact header may be included. The request may be sent compressed.

2) The SS responds to the INVITE request with a 100 Trying response. The response is sent compressed.

3) The SS responds to the INVITE request with a 183 Session in Progress response with the SIP Compression announcement "comp=sigcomp" in the Record-Route header. The response is sent compressed.

4) The SS waits for the UE to send a PRACK request possibly containing the second SDP offer. The SIP Compression announcement "comp=sigcomp" in the Via header may be included and in the Route header shall be included. The request may be sent compressed.

5) The SS responds to the PRACK request with valid 200 OK response. The response is sent compressed.

6) The SS waits for the UE to optionally send a UPDATE request containing the final SDP offer. UE will not send the UPDATE request if PRACK request of step 4 already contained the final offer with preconditions met. The SIP Compression announcement "comp=sigcomp" in the Via header may be included and in the Route header shall be included. The request may be sent compressed.

7) The SS responds to the UPDATE request (if UE sent one) with valid 200 OK response. The response is sent compressed.

8) The SS responds to the INVITE request with 180 Ringing response with the SIP Compression announcement "comp=sigcomp" in the Record-Route header. The response is sent compressed.

9) The SS waits for the UE to send a PRACK request. The SIP Compression announcement "comp=sigcomp" in the Via header may be included and in the Route header shall be included. The request may be sent compressed.

10) The SS responds to the PRACK request with valid 200 OK response. The response is sent compressed.

11) The SS responds to the INVITE request with valid 200 OK response with the SIP Compression announcement "comp=sigcomp" in the Record-Route header. The response is sent compressed.

12) The SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE. The SIP Compression announcement "comp=sigcomp" in the Route shall be included. The acknowledge message may be sent compressed.

13) Call is released on the UE. The SS waits the UE to send a BYE request. The SIP Compression announcement "comp=sigcomp" in the Via header may be included and in the Route header shall be included. The request may be sent compressed.

14) The SS responds to the BYE request with valid 200 OK response. The response is sent compressed.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports. The request may be sent compressed.
2	←		100 Trying	The SS responds with a 100 Trying provisional response. The response is sent compressed.
3	←		183 Session in Progress	The SS responds with an SDP answer indicating the medias and codecs acceptable for SS. The response is sent compressed.
4	→		PRACK	UE acknowledges the receipt of 183 response with PRACK and offers second SDP. The request may be sent compressed.
5	←		200 OK	The SS responds PRACK with 200 OK. The response is sent compressed.
6	→		UPDATE	Optional step: UE sends an UPDATE. The request may be sent compressed.
7	←		200 OK	Optional step: The SS responds UPDATE with 200 OK. The response is sent compressed.
8	←		180 Ringing	The SS responds INVITE with 180. The response is sent compressed.
9	→		PRACK	UE acknowledges the receipt of 180 response by sending PRACK. The request may be sent compressed.
10	←		200 OK	The SS responds PRACK with 200 OK. The response is sent compressed.
11	←		200 OK	The SS responds INVITE with 200 OK to indicate that the virtual remote UE had answered the call. The response is sent compressed.
12	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE. The acknowledge message may be sent compressed.
13	→		BYE	The UE releases the call with BYE. The request may be sent compressed.
14	←		200 OK	The SS sends 200 OK for BYE. The response is sent compressed.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MO call setup" in annex A.2.1.3 with the following exceptions:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp (optional)
Route	
compression-param	comp=sigcomp (optional)
Contact	
compression-param	comp=sigcomp (optional)

100 Trying for INVITE (Step 2)

Use the default message "100 Trying for INVITE" in annex A.2.2.

183 Session in Progress for INVITE (Step 3)

Use the default message “183 Session in Progress for INVITE” in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Record-Route compression-param	The Compression parameter is included in the last route parameter comp=sigcomp

PRACK (Step 4)

Use the default message “PRACK” in annex A.2.4 with the following exceptions:

Header/param	Value/remark
Via via-compression	 comp=sigcomp (optional)
Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp (optional)

200 OK for PRACK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	header shall be present only if there is SDP in message-body *application/sdp*
Content-Length value	 length of message-body
Message-body	SDP body of the 200 response copied from the received PRACK, if it contained one but otherwise omitted. The copied SDP body are modified, but the modifications on SDP body are out of this test case scope.

UPDATE (Step 6) optional step used when PRACK contained a=curr:qos local none

Use the default message “UPDATE” in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Via via-compression	 comp=sigcomp (optional)
Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp (optional)

200 OK for UPDATE (Step 7) - optional step used when UE sent UPDATE

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE but modified. The modifications on SDP body are out of this test case scope.

180 Ringing for INVITE (Step 8)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Record-Route compression-param	The Compression parameter is included in the last route parameter comp=sigcomp

PRACK (Step 9)

Use the default message "PRACK" in annex A.2.4 with the following exceptions:

Header/param	Value/remark
Via via-compression	 comp=sigcomp (optional)
Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp (optional)

200 OK for PRACK (Step 10)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1

200 OK for INVITE (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

ACK (Step 12)

Use the default message "ACK" in annex A.2.7 with the following exceptions:

Header/param	Value/remark
Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp (optional)

BYE (Step 13)

Use the default message "BYE" in annex A.2.8 with the following exceptions:

Header/param	Value/remark
Via via-compression	 comp=sigcomp (optional)
Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp (optional)

200 OK for BYE (Step 14)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

13.2.5 Test requirements

Step 1: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends initial INVITE request as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

...

Step 4: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends a PRACK request as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

...

Step 6: The SS shall check, in the case the UE may conditionally send an UPDATE request and if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 is sent as follows:

a) the message is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

...

Step 9: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends a PRACK request as follows:

a) the message is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

...

Step 12: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends an ACK request as follows:

a) the message is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

Step 13: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends a BYE request as follows:

a) the message is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content.

13.3 SigComp in the MT Call

Editor's note: This test case needs to be updated to Release-8.

13.3.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated call setup when the P-CSCF supports and uses SigComp. This includes correct decompression and compression by the UE.

13.3.2 Conformance requirement

The UE shall support SigComp as specified in RFC 3320. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486.

…

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

…

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

Reference(s)

3GPPTS 24.229 [10], clauses 8.1.1, 8.1.2, and 8.1.3.

13.3.3 Test purpose

1) To verify that, when initiating MT call, the UE performs the session setup according to 3GPP TS 24.229 [10] with compression set to on. The UE can announce to support SIP Compression "comp=sigcomp"; and

2) To verify that the UE decompresses all the SIP messages sent by the SS in accordance 3GPP TS 24.229 [10] clause 8.1.1. This is tested implicitly by verifying the correct exchange of SIP protocol signalling messages.

NOTE: The presence of the SIP Compression announcement "comp=sigcomp" by both UE and P-CSCF indicates the willingness to send or receive SIP messages compressed. The mechanism which controls the willingness to apply SigComp is described in RFC 3486 [26] by sentences containing SHOULD, for this reason the presence of the "comp=sigcomp" parameter from UE side (even if strongly recommended and consistent with the use of compression) is considered optional.

13.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step (with Compression activated on SS).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

1) The SS sends an INVITE request to the UE with the SIP Compression announcement "comp=sigcomp" in the Via header and in the Record-Route header. The request is sent compressed.

2) The SS may receive 100 Trying provisional response from the UE. The Provisional response may be sent compressed.

3) The SS waits for the UE to send a 183 Session Progress provisional response. The SIP Compression announcement "comp=sigcomp" in the Record-Route shall be included and in the Contact header may be included. The Provisional response may be sent compressed.

4) The SS sends PRACK request to the UE to acknowledge the 183 Session Progress with the SIP Compression announcement "comp=sigcomp" in the Via header. The request is sent compressed.

5) The SS waits for the UE to send a 200 OK response for PRACK. The response may be sent compressed.

6) The SS sends UPDATE request to the UE, with SDP indicating that precondition is met on the server side with the SIP Compression announcement "comp=sigcomp" in the Via header. The request is sent compressed.

7) The SS waits for the UE to send a 200 OK response for UPDATE, with proper SDP as answer. The response may be sent compressed.

8) The SS expects and receives 180 Ringing response from the UE. The SIP Compression announcement “comp=sigcomp” in the Contact header may be included. The response may be sent compressed.

9) The SS sends PRACK request with the SIP Compression announcement “comp=sigcomp” in the Via header. The request is sent compressed.

10) The SS waits for the UE to send a 200 OK response for the PRACK. The response may be sent compressed.

11) The SS waits for the UE to send a 200 OK response for the INVITE. The SIP Compression announcement “comp=sigcomp” in the Record-Route shall be included and in the Contact header may be included. The response may be sent compressed.

12) The SS waits for the UE to send the ACK with the SIP Compression announcement “comp=sigcomp” in the Via header. The ACK is sent compressed.

13) The SS sends BYE request to the UE with the SIP Compression announcement “comp=sigcomp” in the Via header. The request is sent compressed.

14) The SS waits for the UE to send a 200 OK response for BYE. The SIP Compression announcement “comp=sigcomp” in the Contact header may be included. The response may be sent compressed.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer. The request is sent compressed.
2	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response. The Provisional response may be sent compressed.
3	→		183 Session Progress	The UE sends 183 response reliably with the SDP answer to the offer in INVITE. The Provisional response may be sent compressed.
4	←		PRACK	SS acknowledges the receipt of 183 from the UE. No SDP offer is included here. The request is sent compressed.
5	→		200 OK	The UE responds to PRACK with 200 OK. The response may be sent compressed.
6	←		UPDATE	SS sends an UPDATE with a second SDP offer after having reserved the resources. The request is sent compressed.
7	→		200 OK	The UE acknowledges the UPDATE with 200 OK and includes SDP answer to acknowledge its current precondition status.
8	→		180 Ringing	The UE responds to INVITE with 180 Ringing after its resource is ready. The response may be sent compressed.
9	←		PRACK	The SS acknowledges the 180 response with PRACK. The request is sent compressed.
10	→		200 OK	The UE acknowledges the PRACK with 200 OK. The response may be sent compressed.
11	→		200 OK	The UE responds to INVITE with 200 OK final response after the user answers the call. The response may be sent compressed.
12	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE. The ACK is sent compressed.
13	←		BYE	The SS sends BYE to release the call. The BYE is sent compressed.
14	→		200 OK	The UE sends 200 OK for the BYE request and ends the call. The response may be sent compressed.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Via via-compression	 comp=sigcomp
Record-Route compression-param	 comp=sigcomp
Message-body	The SDP contains all mandatory SDP lines, as specified in SDP grammar in RFC 4566[27], the details on SDP are out of this test case scope.

100 Trying (Step 2)

Use the default message "100 Trying for INVITE" in annex A.2.2.

183 Session Progress (Step 3)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Record-Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp
Contact compression-param	 comp=sigcomp (optional)
Message-body	Properly generated SDP answer to the SDP offer contained in the INVITE. The details on SDP are out of this test case scope.

PRACK (step 4)

Use the default message "PRACK" in annex A.2.4 with following exceptions:

Header/param	Value/remark
Via via-compression	 Comp=sigcomp
Message-body	Not Present

200 OK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

UPDATE (step 6)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Via via-compression	 Comp=sigcomp (optional)
Message-body	Same SDP offer as in INVITE. The details on SDP are out of this test case scope.

200 OK (step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	 application/SDP
Message-body	Same SDP answer as in 183 Session Progress. The details on SDP are out of this test case scope.

180 Ringing (step 8)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Contact compression-param	 comp=sigcomp (optional)

PRACK (step 9)

Use the default message "PRACK" in annex A.2.4 with following exceptions:

Header/param	Value/remark
Via via-compression	 comp=sigcomp
Message-body	Not Present

200 OK (step 10)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

200 OK (step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with following exceptions:

Header/param	Value/remark
Contact compression-param	 comp=sigcomp (optional)

ACK (step 12)

Use the default message "ACK" in annex A.2.7 with following exceptions:

Header/param	Value/remark
Via via-compression	 comp=sigcomp

BYE (step 13)

Use the default message "BYE" in annex A.2.8 with following exceptions:

Header/param	Value/remark
Via via-compression	 comp=sigcomp

200 OK (step 14)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with following exceptions:

Header/param	Value/remark
Contact	
compression-param	comp=sigcomp (optional)

13.3.5 Test requirements

Step 2 (optional step): The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 100 Trying response as follow:

a) the request is sent compressed according to RFC 3320 [24]; and

Step 3: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 183 Session Progress response as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent request and response compressed the message content shall be in accordance to the specific message content; and

...

Step 5: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follow:

a) the request is sent compressed according to RFC 3320 [24]; and

Step 7: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follow:

a) the request is sent compressed according to RFC 3320 [24]; and

Step 8: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 180 Ringing response as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent request and response compressed the message content shall be in accordance to the specific message content; and

...

Step 10: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follow:

a) the request is sent compressed according to RFC 3320 [24]; and

Step 11: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent request and response compressed the message content shall be in accordance to the specific message content; and

...

Step 14: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent request and response compressed the message content shall be in accordance to the specific message content.

13.4 Void

14 Emergency Service

14.1 Void

14.2 Void

15 Supplementary Services

15.1 Originating Identification Presentation

15.1.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Originating Identification Presentation. This process is described in 3GPP TS 24.607 [102].

15.1.2 Conformance requirement

Generic requirements for Originating Identification Presentation can be found from Annexes F.1 and F.2.

[TS 24.607 clause 4.2.1]:

The OIP service provides the terminating user with the possibility of receiving trusted (i.e. network provided) identity information in order to identify the originating user.

In addition to the trusted identity information, the identity information from the originating user can include identity information generated by the originating user and in general transparently transported by the network. In the particular case where the "no screening" special arrangement does not apply, the originating network shall verify the content of this user generated identity information. The terminating network cannot be responsible for the content of this user generated identity information.

[TS 24.607 clause 4.10.1]:

The OIP service can be activated/deactivated using the active attribute of the <originating-identity-presentation> service element.

Reference(s)

3GPP TS 24.607[102], clauses 4.2.1 and 4.10.1.

15.1.3 Test purpose

1) To verify that the UE can request activation of Originating Identification Presentation with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Originating Identification Presentation; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Originating Identification Presentation, at step 7 deactivation of Originating Identification Presentation is respectively triggered at the UE.

15.1.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2, NOTE 1) or

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <originating-identity-presentation> element with "active" attribute set as "true" or with “active” attribute not present.

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <originating-identity-presentation> element with "active" attribute being set "false"

15.2 Originating Identification Restriction

15.2.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Originating Identification Restriction. This process is described in 3GPP TS 24.607 [102].

15.2.2 Conformance requirement

Generic requirements for Originating Identification Restriction can be found from Annexes F.1 and F.2.

[TS 24.607 clause 4.2.1]:

The OIR service is a service offered to the originating user. It restricts presentation of the originating user's identity information to the terminating user.

When the OIR service is applicable and activated, the originating network provides the destination network with the indication that the originating user's identity information is not allowed to be presented to the terminating user. In this case, no originating user's identity information shall be included in the requests sent to the terminating user. The presentation restriction function shall not influence the forwarding of the originating user's identity information within the network as part of the simulation service procedures.

[TS 24.607 clause 4.10.1]:

The OIR service can be activated/deactivated using the active attribute of the <originating-identity-presentation-restriction> service element. Activating the OIR service this way activates the temporary mode OIR service. When deactivated and not overruled by operator settings, basic communication procedures apply.

Reference(s)

3GPP TS 24.607 [102], clauses 4.2.1 and 4.10.1.

15.2.3 Test purpose

1) To verify that the UE can request activation of Originating Identification Restriction with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Originating Identification Restriction; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Originating Identification Restriction, at step 7 deactivation of Originating Identification Restriction is respectively triggered at the UE.

15.2.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <originating-identity-presentation-restriction> element with "active" attribute set as "true" or with “active” attribute not present.

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <originating-identity-presentation-restriction> element with "active" attribute being set "false"

15.2a Originating Identification Restriction / Signalling

15.2a.1 Definition

Test to verify that the UE correctly invokes the IMS Multimedia Telephony Originating Identification Restriction in temporary mode. This process is described in 3GPP TS 24.607 [102].

15.2a.2 Conformance requirement

Generic requirements for Originating Identification Restriction can be found in Annex F.2.

[TS 24.607 clause 4.5.2.1]:

If the originating user wishes to override the default setting of "presentation not restricted" of the OIR service in temporary mode:

- The originating UE shall include an "anonymous" From header field. The convention for configuring an anonymous From header field described in IETF RFC 3323 [6] should be followed; i.e. From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag= xxxxxxx.
- If only the P-Asserted-Identity needs to be restricted the originating UE shall include a Privacy header field [6] set to "id" in accordance with IETF RFC 3325 [7].
- If all headers containing private information that the UE cannot anonymize itself need to be restricted, the originating UE shall include a Privacy header field set to "header" in accordance with IETF RFC 3323 [6].

NOTE 2: The Privacy header field value "header" does not apply to the identity in the From header field.

Reference(s)

3GPP TS 24.607 [102], clause 4.5.2.1.

15.2a.3 Test purpose

To verify that the UE sends an INVITE with the correct headers when initiating an IMS call with originating identification restriction in temporary mode and wanting to restrict presentation of

- the From and P-Asserted-Identity headers., or
- all headers containing private information that the UE cannot anonymize itself

15.2a.4 Method of test

Same as clause 12.12 with the following exceptions.

Initial conditions

Same as clause 12.12 with the following addition:

The UE is configured to use Originating Identification Restriction in temporary mode. The corresponding default is set to “presentation not restricted”

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS speech call with originating identification restriction	
2-13			Steps 2 to 13 defined in annex C.21	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
14			Steps defined in annex C.32	Generic test procedure for MO release of IMS call

Specific Message Contents

Steps 2 - 13 as specified in annex C.21 with the following exceptions:

INVITE (Step 2)

Header/param	Value/remark	Reference
From		
addr-spec	*"Anonymous" <sip:anonymous@anonymous.invalid>*	
Privacy	*id* or *header* (mutually exclusive)	RFC 3323 [135] RFC 3325 [89]

15.2a.5 Test requirements

Step 2: The UE shall send the INVITE request including the following headers:

From header: "Anonymous" <sip:anonymous@anonymous.invalid>

Privacy header: id or header

15.3 Terminating Identification Presentation

15.3.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Terminating Identification Presentation. This process is described in 3GPP TS 24.608 [103].

15.3.2 Conformance requirement

[TS 24.608 clause 4.2.1]:

The Terminating Identification Presentation (TIP) service provides the originating party with the possibility of receiving trusted information in order to identify the terminating party.

[TS 24.608 clause 4.9.1]:

The TIP service can be activated/deactivated using the active attribute of the <terminating-identity-presentation> service element.

Reference(s)

3GPP TS 24.608 [103], clauses 4.2.1 and 4.9.1.

15.3.3 Test purpose

1) To verify that the UE can request activation of Terminating Identification Presentation with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Terminating Identification Presentation; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Terminating Identification Presentation, at step 7 deactivation of Terminating Identification Presentation is respectively triggered at the UE.

15.3.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <terminating-identity-presentation> element with "active" attribute set as "true" or with “active” attribute not present.

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <terminating-identity-presentation> element with "active" attribute being set "false"

15.4 Terminating Identification Restriction

15.4.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Terminating Identification Restriction. This process is described in 3GPP TS 24.608 [103].

15.4.2 Conformance requirement

[TS 24.608 clause 4.2.1]:

The Terminating Identification Restriction (TIR) is a service offered to the terminating party which enables the terminating party to prevent presentation of the terminating identity information to originating party.

[TS 24.608 clause 4.9.1]:

The TIR service can be activated/deactivated using the active attribute of the <terminating-identity-presentation-restriction> service element. Activating the TIR service this way activates the temporary mode TIR service. When deactivated and not overruled by operator settings, basic communication procedures apply.

Reference(s)

3GPP TS 24.608 [103], clauses 4.2.1 and 4.9.1.

15.4.3 Test purpose

1) To verify that the UE can request activation of Terminating Identification Restriction with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Terminating Identification Restriction; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.4.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Terminating Identification Restriction, at step 7 deactivation of Terminating Identification Restriction is respectively triggered at the UE.

15.4.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <terminating-identity-presentation-restriction> element with "active" attribute set as "true" or with “active” attribute not present.

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <terminating-identity-presentation-restriction> element with "active" attribute being set "false"

15.4a Terminating Identification Restriction / Signalling

15.4a.1 Definition

Test to verify that the UE correctly invokes the IMS Multimedia Telephony Terminating Identification Restriction in temporary mode. This process is described in 3GPP TS 24.608 [103].

15.4a.2 Conformance requirement

Generic requirements for Originating Identification Restriction can be found in Annex F.3.

[TS 24.608 clause 4.2.1]:

The Terminating Identification Restriction (TIR) is a service offered to the terminating party which enables the terminating party to prevent presentation of the terminating identity information to originating party.

[TS 24.608 clause 4.5.2.12]:

The destination UE, if the terminating user wishes to override the default setting of "presentation not restricted" of the TIR service in temporary mode, shall include a Privacy header with privacy type of "id" in any non-100 responses it sends upon receipt of a SIP request.

….NOTE: It is assumed that TIR subscribers support IETF RFC 3325.

Reference(s)

3GPP TS 24.608 [103], clauses 4.2.1 and 4.5.2.12.

15.4a.3 Test purpose

To verify that the UE includes a Privacy header with privacy type of "id" in any non-100 responses it sends upon receipt of a SIP request when using the TIR service in temporary mode and the terminating user wishing to override the default setting currently set to “not restricted”

15.4a.4 Method of test

Same as clause 12.13 with the following exceptions.

Initial conditions

Same as clause 12.13 with the following addition:

The UE is configured to use Terminating Identification Restriction in temporary mode. The corresponding default is currently set to “presentation not restricted”.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-11			Steps 1-11 defined in annex C.11	MTSI MT speech call. Referred from 36.508 [94] table 4.5A.7.3-1 for a UE with E-UTRA support.
12				Make UE accept the MTSI MT speech offer with Terminating Identification Restriction
13-16			Steps 12-15 defined in annex C.11	MTSI MT speech call. Referred from 36.508 [94] table 4.5A.7.3-1 for a UE with E-UTRA support.

Specific Message Contents

Steps 1-11 and 13-16 as specified in annex C.11 with the following exceptions:

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark	Reference
Privacy	*id*	RFC 3323 [135] RFC 3325 [89]

180 Ringing (Step 9)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following exceptions:

Header/param	Value/remark	Reference
Privacy	*id*	RFC 3323 [135] RFC 3325 [89]

200 Ok (Step 12)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark	Reference
Privacy	*id*	RFC 3323 [135] RFC 3325 [89]

15.4a.5 Test requirements

Steps 4, 9 and 12: The UE shall include a Privacy header with privacy type set to "id".

15.5 Communication Forwarding unconditional

15.5.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding unconditional. This process is described in 3GPP TS 24.604 [106].

15.5.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F.1 and F.4.

[TS 24.604, clause 4.2.1.2]:

The CFU service enables a served user to have the network redirect to another user communications which are addressed to the served user's address. The CFU service may operate on all communication, or just those associated with specified services. The served user's ability to originate communications is unaffected by the CFU supplementary service. After the CFU service has been activated, communications are forwarded independent of the status of the served user.

As a service provider option, a subscription option can be provided to enable the served user to receive an indication that the CFU service has been activated. This indication shall be provided when the served user originates a communication if the CFU service has been activated for the served user's address and for the service requested for the communication.

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106].

15.5.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding unconditional with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding unconditional; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Communication Forwarding unconditional;

At step 5b, when sending 200 OK for GET, SS delivers a simservs document as specified in TS 24.604 [106] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <communication-diversion active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
               <cp:conditions>
                  <no-answer/>
                  <rule-deactivated/>
               </cp:conditions>
               <cp:actions>
                   <forward-to>
                       <target>
                          px_XCAP_TargetUri
                       </target>
                       <notify-caller>true</notify-caller>
                   </forward-to>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </communication-diversion>
</simservs>
```

At step 7 deactivation of Communication Forwarding unconditional is respectively triggered at the UE.

15.5.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme it supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element missing or empty as forwarding is supposed to be unconditional and not containing a <rule-deactivated> element
    - <cp:actions> element containing <forward-to> element containing <target> element
      - value of target address to be px_XCAP_TargetUri

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

or

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element found at step 2 for Communication Forwarding unconditional as follows:
    - <cp:conditions> element containing a <rule-deactivated> element

15.6 Void

15.7 Communication Forwarding on non Reply: activation

15.7.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user does not answer to the phone. This process is described in 3GPP TS 24.604 [106].

15.7.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F.1 and F.4.

[TS 24.604, clause 4.2.1.4]:

The CFNR service enables a served user to have the network redirect to another user communications which are addressed to the served user's address, and for which the connection is not established within a defined period of time. The CFNR service may operate on all communications, or just those associated with specified services. The served user's ability to originate communications is unaffected by the CFNR supplementary service.

The CFNR service can only be invoked by the network after the communication has been offered to the served user and an indication that the called user is being informed of the communication has been received.

As a service provider option, a subscription option can be provided to enable the served user to receive an indication that the CFNR service has been activated. This indication shall be provided when the served user originates a communication if the CFNR service has been activated for the served user's address and for the service requested for the communication.

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106]

15.7.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding (when the called user does not answer) with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.7.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Communication Forwarding on non Reply;

At step 5b, SS delivers a simservs document as specified in TS 24.604 [106] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <communication-diversion active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
               <cp:conditions>
                  <no-answer/>
                  <rule-deactivated/>
               </cp:conditions>
               <cp:actions>
                   <forward-to>
                       <target>
                          px_XCAP_TargetUri
                       </target>
                       <notify-caller>true</notify-caller>
```

```
                    </forward-to>
                </cp:actions>
            </cp:rule>
          </cp:ruleset>
    </communication-diversion>
 </simservs>
```

At step 7 deactivation of Communication Forwarding on non Reply is respectively triggered at the UE.

15.7.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2, NOTE 1) or
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).-

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
    - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
        - <cp:conditions> element containing a <no-answer> element and not containing a <rule-deactivated> element
        - <cp:actions> element containing <forward-to> element containing <target> element. Additionally <NoReplyTimer> element shall be included, if the UE supports no reply timer setting.
- value of target address to be px_XCAP_TargetUri
- value of NoReplyTimer (if included) to be 10 seconds

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

or

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
    - within <cp:ruleset> one <cp:rule> element found at step 2 for communication forwarding as follows:
        - <cp:conditions> element containing a <rule-deactivated> element

15.8 Communication Forwarding on non reply: MO call initiation

15.8.1 Definition

Test to verify that the MTSI MO UE correctly handles session setup where call is being forwarded due to no reply. This process is described in 3GPP TS 24.604 [106], clauses 4.2.1, 4.5.2.1 and A.1.3 and 3GPP TS 24.229 [10], clause 9.2.3.

15.8.2 Conformance requirement

[TS 24.604, clause 4.2.1.4]:

The CFNR service enables a served user to have the network redirect to another user communications which are addressed to the served user's address, and for which the connection is not established within a defined period of time. The CFNR service may operate on all communications, or just those associated with specified services. The served user's ability to originate communications is unaffected by the CFNR supplementary service.

The CFNR service can only be invoked by the network after the communication has been offered to the served user and an indication that the called user is being informed of the communication has been received.

[TS 24.604, clause 4.5.2.1]:

When communication diversion has occurred on the served user side and the network option "*Originating*" user receives notification that his communication has been diverted (forwarded or deflected)" is set to true, the originating UA may receive a 181 (Call is being forwarded) response according to the procedures described in 3GPP TS 24.229.

The Information given by the History header could be displayed by the UA if it is a UE.

[TS 24.229, clause 9.2.3]:

Since the UE does not know that forking has occurred until a second provisional response arrives, the UE will request the radio/bearer resources as required by the first provisional response. For each subsequent provisional response that may be received, different alternative actions may be performed depending on the requirements in the SDP answer:

- the UE has sufficient radio/bearer resources to handle the media specified in the SDP of the subsequent provisional response, or
- the UE must request additional radio/bearer resources to accommodate the media specified in the SDP of the subsequent provisional response.

NOTE 1: When several forked responses are received, the resources requested by the UE is the "logical OR" of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 2: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When an 199 (Early Dialog Terminated) response for the INVITE request is received for an early dialogue, the UE shall release reserved radio/bearer resources associated with that early dialogue.

When the first final 200 (OK) response for the INVITE request is received for one of the early dialogues, the UE proceeds to set up the SIP session using the radio/bearer resources required for this session. Upon the reception of the first final 200 (OK) response for the INVITE request, the UE shall release all unneeded radio/bearer resources.

GIBA:

NOTE 1: GIBA does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

Reference(s)

3GPP TS 24.604 [106], clauses 4.2.1 and 4.5.2.1; 3GPP TS 24.229 [10], clause 9.2.3

15.8.3 Test purpose

1) To verify that when initiating MO call the UE handles correctly the successive 180 and 181 provisional responses received during call setup.

15.8.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-9B) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 but only steps 1 to 11 of Annex C.21 in the parallel behaviour to steps 13-14 of table 4.5A.6.3-1.

10) SS responds to the INVITE with a valid 181 Call Is Being Forwarded response.

11) SS (now starting to simulate the UE to which call was forwarded) sends another 183 Session in Progress response to the INVITE request. As this response contains an SDP answer it is sent reliably.

12) SS waits for the UE to send a PRACK request, containing an SDP offer in which the UE tells to have reserved the local resources.

13) SS responds to the PRACK request with valid 200 OK response. The response contains an SDP answer which tells that SS has reserved its local resources as well.

13A) UE may send an UPDATE request.

13B) If UE sent and UPDATE request, SS responds with 200 OK.

14) SS responds to the INVITE request with 180 Ringing response.

14A) As the 180 Ringing response was sent reliably, UE sends a PRACK request.

14B) SS responds to PRACK with 200 OK.

15) SS responds to the INVITE request with valid 200 OK response.

16) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

17) Call is released on the UE. SS waits the UE to send a BYE request.

18) SS responds to the BYE request with valid 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-9B			Steps 1-11 as defined in Annex C.21	The same messages as in steps 2 - 11 of Annex C.21 are used. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
10	←		181 Call is being forwarded	SS sends 181 response to indicate that call forwarding has been started as the user did not answer to the phone
11	←		183 Session Progress	SS (simulating the phone to which the call was forwarded) responds with 183 Session Progress containing an SDP answer indicating support for AMR-WB codec and state of the local preconditions. UE will consider this response as forked one since it has different To tag this time compared to step 8.
12-13B			Steps 5-8 as defined in Annex C.21	The same messages as specified in steps 5 - 8 of Annex C.21 are used with To-tag and Contact Address as in the 183 response of step 11
14	←		180 Ringing	The SS sends 180 Ringing response to the UE
14A	→		PRACK	UE acknowledges the receipt of 180 response by sending PRACK.
14B	←		200 OK	The SS responds PRACK with 200 OK.
15	←		200 OK	The SS responds INVITE with 200 OK to indicate that the virtual remote UE had answered the call
16	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
17	→		BYE	The UE releases the call with BYE
18	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable

Specific Message Contents

181 Call is being forwarded for INVITE (Step 10)

Use the default message “181 Call is being forwarded” in annex A.2.14

183 Session Progress for INVITE (Step 11)

Use the default message “183 Session in Progress for INVITE” in annex A.2.3 with the following exceptions:

Header/param	Value/remark
To tag	 different tag must be used than the one used in steps 3-9 as this response is now from another UE and belongs to another dialog instance. Note that this new tag must be used within the rest of the steps (10-17) in this test case instead of the tag used within steps 3-9.
Contact addr-spec	 different URI must be used than the one used in step 3 as this is supposed now to represent another UE to which the call is being forwarded.. Note that this new Contact must be used within the rest of the steps (13-14) in this test case.
Require option-tag	 *precondition*
Message-body	Same contents as specified in step 4 annex C.21. except for o-line: *o=- 22222222 22222222 IN* (addrtype) (unicast-address for new remote UE).

PRACK or UPDATE (Step 12 or 13A)

The UE shall include an SDP body as described in C.21, Step 5 , but with the following exceptions:

- Contents of o= line is not checked

180 Ringing for INVITE (Step 14)

Use the default message “180 Ringing for INVITE” in annex A.2.6 applying condition A3 (Response sent reliably) and with the following exceptions:

Header/param	Value/remark
Contact addr-spec	 Same value as in the 183 response of step 11
History-Info hi-targeted-to-uri hi-index	 Same value as in the 181 response of step 10 Same value as in the 181 response of step 10

PRACK (Step 14A)

Use the default message “PRACK” in annex A.2.4.

200 OK for PRACK (Step 14B)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

200 OK for INVITE (Step 15)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	Same value as in the 183 response of step 11
History-Info	
hi-targeted-to-uri	Same value as in the 181 response of step 10
hi-index	Same value as in the 181 response of step 10

ACK (Step 16)

Use the default message “ACK” in annex A.2.7.

BYE (Step 17)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 18)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

15.8.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.9 Communication Forwarding on Busy

15.9.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is busy. This process is described in 3GPP TS 24.604 [106].

15.9.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F.1 and F.4.

[TS 24.604, clause 4.2.1.3]:

The CFB service enables a served user to have the network redirect to another user communications which are addressed to the served user's address and meet busy. The CFB service may operate on all communications, or just those associated with specified services. The served user's ability to originate communications is unaffected by the CFB supplementary service.

As a service provider option, a subscription option can be provided to enable the served user to receive an indication that the CFB service has been activated. This indication shall be provided when the served user originates a communication if the CFB service has been activated for the served user's address and for the service requested for the communication.

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106]

15.9.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding (when the called user is busy) with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.9.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Communication Forwarding on Busy;

At step 5b, SS delivers a simservs document as specified in TS 24.604 [106] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <communication-diversion active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
               <cp:conditions>
                   <busy/>
                   <rule-deactivated/>
               </cp:conditions>
               <cp:actions>
                   <forward-to>
                       <target>
                          px_XCAP_TargetUri
                       </target>
                       <notify-caller>true</notify-caller>
                   </forward-to>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </communication-diversion>
</simservs>
```

At step 7 deactivation of Communication Forwarding on Busy is respectively triggered at the UE.

15.9.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element containing a <busy> element and not containing a <rule-deactivated>
    - <cp:actions> element containing <forward-to> element containing <target> element
- value of target address to be px_XCAP_TargetUri

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

or

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element found at step 2 for communication forwarding as follows:
    - <cp:conditions> element containing a <rule-deactivated> element

15.10 Communication Forwarding on Not logged-in

15.10.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is not registered to IMS service. This process is described in 3GPP TS 24.604 [106].

15.10.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F.1 and F.4.

[TS 24.604, clause 4.2.1.7]:

The Communication Forwarding on Not Logged-in (CFNL) service enables a served user to redirect incoming communications which are addressed to the served user's address, to another user (forwarded-to address) in case the served user is not registered (logged-in). The CFNL service may operate on all communications, or just those associated with specified basic services.

As a service provider option, a subscription option can be provided to enable the served user to receive an indication that the CFNL service has been activated. This indication shall be provided when the served user logs out according to procedures described in RFC 3261

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106]

15.10.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding (when the called user is not logged in) with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.10.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Communication Forwarding on Not logged-in;

At step 5b, SS delivers a simservs document as specified in TS 24.604 [106] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <communication-diversion active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
               <cp:conditions>
                    <not-registered/>
                    <rule-deactivated/>
               </cp:conditions>
               <cp:actions>
                   <forward-to>
                       <target>
                          px_XCAP_TargetUri
                       </target>
                       <notify-caller>true</notify-caller>
                   </forward-to>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </communication-diversion>
</simservs>
```

At step 7 deactivation of Communication Forwarding on Not logged-in is respectively triggered at the UE.

15.10.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element containing a <not-registered> element and not containing a <rule-deactivated> element
    - <cp:actions> element containing <forward-to> element containing <target> element
      - value of target address to be px_XCAP_TargetUri

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

or

- <communication-diversion> element with "active" attribute being set "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element found at step 2 for Communication Diversion as follows:
    - <cp:conditions> element containing a <rule-deactivated> element

15.10a Communication Forwarding on Not reachable

15.10a.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is not reachable. This process is described in 3GPP TS 24.604 [106].

15.10a.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F.1 and F.4.

[TS 24.604]:

Communication Forwarding on Subscriber Not Reachable (CFNRc)

The CFNRc service enables an user to have the network redirect all incoming communications, when the user is not reachable (e.g. there is no IP connectivity to the user's terminal), to another user. The CFNRc service may operate on all communications, or just those associated with specified services. The user's ability to originate communications is unaffected by the CFNRc simulation service.

As a service provider option, a subscription option can be provided to enable the user to receive an indication that the CFNRc service has been activated. This indication may be provided when the user originates a communication if the CFNRc service has been activated for the user and for the service requested for the communication.

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106]

15.10a.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding (when the called user is not reachable) with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.10a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Communication Forwarding on Not reachable;

At step 5b, SS delivers a simservs document as specified in TS 24.604 [106] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <communication-diversion active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
               <cp:conditions>
                    <not-reachable/>
                    <rule-deactivated/>
               </cp:conditions>
               <cp:actions>
                   <forward-to>
                       <target>
                          px_XCAP_TargetUri
                       </target>
                       <notify-caller>true</notify-caller>
                   </forward-to>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </communication-diversion>
</simservs>
```

At step 7 deactivation of Communication Forwarding on Not reachable is respectively triggered at the UE.

15.10a.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element containing a <not-reachable> element and not containing a <rule-deactivated> element
    - <cp:actions> element containing <forward-to> element containing <target> element
      - value of target address to be px_XCAP_TargetUri

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

or

- <communication-diversion> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element found at step 2 for communication forwarding as follows:
    - <cp:conditions> element containing a <rule-deactivated> element

15.11 MO Call Hold without announcement

15.11.1 Definition

Test to verify that the UE correctly performs IMS mobile originated call hold and resume. This process is described in 3GPP TS 24.610 [108].

15.11.2 Conformance requirement

[TS 24.610 clause 4.5.2.1]:

In addition to the application of procedures according to 3GPP TS 24.229, the following procedures shall be applied at the invoking UE in accordance with RFC 3264.

If individual media streams are affected, the invoking UE shall generate a new SDP offer where:

- for each media stream that is to be held, the SDP offer that contains:
  - an "inactive" SDP attribute if the stream was previously set to "recvonly" media stream; or
  - a "sendonly" SDP attribute if the stream was previously set to "sendrecv" media stream;
- for each media stream that is to be resumed, the SDP offer contains:
  - a "recvonly" SDP attribute if the stream was previously an inactive media stream; or

- a "sendrecv" SDP attribute if the stream was previously a sendonly media stream, or the attribute may be omitted, since sendrecv is the default; or

- for each media stream that is unaffected, the media parameters in the SDP offer remain unchanged from the previous SDP offer.

If all the media streams are to be held, the invoking UE shall generate an SDP offer containing a session level direction attribute, or separate media level direction attributes, in the SDP that is set to:

- "inactive" if the streams were previously set to "recvonly" media streams; or

- "sendonly" if the streams were previously set to "sendrecv" media streams; or

If all the media streams that shall be resumed, the invoking UE shall generate a session level direction attribute, or separate media level direction attributes, in the SDP that is set to:

- "recvonly" if the streams were previously inactive media streams; or

- "sendrecv" if the streams were previously sendonly media streams, or the attribute may be omitted, since sendrecv is the default.

Then the UE shall send the generated SDP offer in a re-INVITE request (or UPDATE request) to the remote UE.

[TS 26.114 clause 7.3.1]:

RTCP packets should be sent for all types of multimedia sessions to enable synchronization with other RTP transported media, remote end-point aliveness information, monitoring of the transmission quality, and carriage of feedback messages such as TMMBR for video and RTCP APP for speech. Point-to-point speech only sessions may not require these functionalities and may therefore turn off RTCP by setting the SDP bandwidth modifiers (RR and RS) to zero. When RTCP is turned off (for point-to-point speech only sessions) and the media is put on hold, the MTSI client should re-negotiate the RTCP bandwidth with SDP bandwidth modifiers values greater than zero, and send RTCP packets to the other end. This allows the remote end to detect link aliveness during hold. When media is resumed, the resuming MTSI client should turn off the RTCP sending again through a re-negotiation of the RTCP bandwidth with SDP bandwidth modifiers equal to zero.

[TS 24.229 clause 6.1.1]:

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in or 3GPP 29.213.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

Reference(s)

3GPP TS 24.610 [108], 3GPP TS 24.229 [10]

15.11.3 Test purpose

1) To verify that the invoking UE puts the call on hold with a correct exchange of SIP/SDP protocol signalling messages; and

2) To verify that the invoking UE is able to resume the call with a correct exchange of SIP/SDP protocol signalling messages.

15.11.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Test procedure

1) Call hold is initiated on the UE. SS waits for the UE to send an INVITE or UPDATE request with a SDP offer
2) If the UE sent an INVITE request in step 1, SS responds to it with a 100 Trying response. No such response is sent for UPDATE.
3) SS responds to the INVITE or UPDATE request with a valid 200 OK response.
4) If the UE sent an INVITE request in step 1, SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.
5) Call resume is initiated on the UE. SS waits for the UE to send an INVITE or UPDATE request with a SDP offer
6) If the UE sent an INVITE request in step 5, SS responds to it with a 100 Trying response. No such response is sent for UPDATE.
7) SS responds to the INVITE or UPDATE request with a valid 200 OK response.
8) If the UE sent an INVITE in step 5, SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.
9) Call is released on the UE. SS waits for the UE to send a BYE request.
10) SS responds to the BYE request with valid a 200 OK response.

Expected sequence

Step	Direction UE	Direction SS	Message	Comment
			User initiates holding the call	
1-4			Steps 1-4 specified in annex C.8 to hold the call	
			User initiates resuming the call	
5-8			Steps 1-4 specified in annex C.8 to resume the call	
			User initiates releasing the call	
9	→		BYE	The UE releases the call with BYE
10	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Messages in Step 1-4

Use messages according to annex C.8 to put the call on hold.

Messages in Step 5-8

Use messages according to annex C.8 to resume the call.

15.11.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 1: the UE shall send an INVITE or UPDATE request with correct content. The UE shall include the same lines in the SDP body as specified call hold in step 1 of annex C.8.

Step 5: the UE shall send an INVITE or UPDATE request with correct content. The UE shall include the same lines in the SDP body as specified for call resume in step 1 of annex C.8.

15.11a MO Video Call Hold without announcement

15.11a.1 Definition

Test to verify that the UE correctly performs IMS mobile originated video call hold and resume. This process is described in 3GPP TS 24.610 [108].

15.11a.2 Conformance requirement

[TS 24.610 clause 4.5.2.1]:

In addition to the application of procedures according to 3GPP TS 24.229 [1] , the following procedures shall be applied at the invoking UE in accordance with RFC 3264 [4].

A UE shall not invoke the HOLD service on a dialog associated with an emergency call the UE has initiated.

If individual media streams are affected, the invoking UE shall generate a new SDP offer where:

- for each media stream that is to be held, the SDP offer that contains:
  - an "inactive" SDP attribute if the stream was previously set to "recvonly" media stream; or
  - a "sendonly" SDP attribute if the stream was previously set to "sendrecv" media stream;
- for each media stream that is to be resumed, the SDP offer contains:
  - a "recvonly" SDP attribute if the stream was previously an inactive media stream; or
  - a "sendrecv" SDP attribute if the stream was previously a sendonly media stream, or the attribute may be omitted, since sendrecv is the default; or
- for each media stream that is unaffected, the media parameters in the SDP offer remain unchanged from the previous SDP offer.

If all the media streams are to be held, the invoking UE shall generate an SDP offer containing a session level direction attribute, or separate media level direction attributes, in the SDP that is set to:

- "inactive" if the streams were previously set to "recvonly" media streams; or
- "sendonly" if the streams were previously set to "sendrecv" media streams; or

If all the media streams that shall be resumed, the invoking UE shall generate a session level direction attribute, or separate media level direction attributes, in the SDP that is set to:

- "recvonly" if the streams were previously inactive media streams; or
- "sendrecv" if the streams were previously sendonly media streams, or the attribute may be omitted, since sendrecv is the default.

Then the UE shall send the generated SDP offer in a re-INVITE request (or UPDATE request) to the remote UE.

[TS 26.114 clause 7.3.1]:

RTCP packets should be sent for all types of multimedia sessions to enable synchronization with other RTP transported media, remote end-point aliveness information, monitoring of the transmission quality, and carriage of feedback messages such as TMMBR for video and RTCP APP for speech. Point-to-point speech only sessions may not require these functionalities and may therefore turn off RTCP by setting the SDP bandwidth modifiers (RR and RS) to zero. When RTCP is turned off (for point-to-point speech only sessions) and the media is put on hold, the MTSI client should re-negotiate the RTCP bandwidth with SDP bandwidth modifiers values greater than zero, and send RTCP packets to the other end. This allows the remote end to detect link aliveness during hold. When media is resumed, the resuming MTSI client should turn off the RTCP sending again through a re-negotiation of the RTCP bandwidth with SDP bandwidth modifiers equal to zero.

[TS 24.229 clause 6.1.1]:

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in or 3GPP 29.213.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

Reference(s)

3GPP TS 24.610 [108], 3GPP TS 24.229 [10]

15.11a.3 Test purpose

1) To verify that the invoking UE puts the call on hold with a correct exchange of SIP/SDP protocol signalling messages; and

2) To verify that the invoking UE is able to resume the call with a correct exchange of SIP/SDP protocol signalling messages.

15.11a.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.8.3-1, steps 1 to 15.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO Video call.

Test procedure

1) Call hold is initiated on the UE. SS waits for the UE to send an INVITE or UPDATE request with a SDP offer

2) If the UE sent an INVITE request in step 1, SS responds to it with a 100 Trying response. No such response is sent for UPDATE.

3) SS responds to the INVITE or UPDATE request with a valid 200 OK response.

4) If the UE sent an INVITE request in step 1, SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

5) Call resume is initiated on the UE. SS waits for the UE to send an INVITE or UPDATE request with a SDP offer

6) If the UE sent an INVITE request in step 5, SS responds to it with a 100 Trying response. No such response is sent for UPDATE.

7) SS responds to the INVITE or UPDATE request with a valid 200 OK response.

8) If the UE sent an INVITE in step 5, SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

9) Call is released on the UE. SS waits for the UE to send a BYE request.

10) SS responds to the BYE request with valid a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
			User initiates holding the call	
1-4			Steps 1-4 specified in annex C.8 to hold the call	
			User initiates resuming the call	
5-8			Steps 1-4 specified in annex C.8 to resume the call	
			User initiates releasing the call	
9	→		BYE	The UE releases the call with BYE
10	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Messages in Step 1-4

Use messages according to annex C.8 to put the call on hold.

Messages in Step 5-8

Use messages according to annex C.8 to resume the call.

15.11a.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 1: the UE shall send an INVITE or UPDATE request with correct content. The UE shall include the same lines in the SDP body as specified call hold in step 1 of annex C.8.

Step 5: the UE shall send an INVITE or UPDATE request with correct content. The UE shall include the same lines in the SDP body as specified for call resume in step 1 of annex C.8.

15.12 MT Call Hold without announcement

15.12.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated call hold and resume. This process is described in 3GPP TS 24.610 [108].

15.12.2 Conformance requirement

[TS 24.610 clause 4.5.2.9]:

Basic communication procedures according to TS 24.229 shall apply.

[TS 24.229 clause 6.1.1]:

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in or 3GPP 29.213.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent; therefore, the RR bandwidth modifier will typically get the value of zero.

[TS 26.114 clause 7.3.1]:

RTCP packets should be sent for all types of multimedia sessions to enable synchronization with other RTP transported media, remote end-point aliveness information, monitoring of the transmission quality, and carriage of feedback messages such as TMMBR for video and RTCP APP for speech. Point-to-point speech only sessions may not require these functionalities and may therefore turn off RTCP by setting the SDP bandwidth modifiers (RR and RS) to zero. When RTCP is turned off (for point-to-point speech only sessions) and the media is put on hold, the MTSI client should re-negotiate the RTCP bandwidth with SDP bandwidth modifiers values greater than zero, and send RTCP packets to the other end. This allows the remote end to detect link aliveness during hold. When media is resumed, the resuming MTSI client should turn off the RTCP sending again through a re-negotiation of the RTCP bandwidth with SDP bandwidth modifiers equal to zero.

Reference(s)

3GPP TS 24.610 [108], TS 24.229 [10]

15.12.3 Test purpose

1) To verify that the held UE responds correctly to call hold and resume requests from SS.

15.12.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Test procedure

1) SS initiates the call hold by sending a re-INVITE to set the media streams into sendonly state.

2) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.

3) SS waits for the UE to respond to the INVITE request with valid 200 OK response.

4) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE.

5) SS resumes the call by sending another re-INVITE request with a SDP offer to set the media streams into sendrecv state again.

6) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.

7) SS waits for the UE to respond to the INVITE request with valid 200 OK response.

8) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE.

9) SS sends a BYE request to the UE in order to release the call.

10) UE responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-4			Steps 1-4 specified in annex C.9 to hold the call	
5-8			Steps 1-4 specified in annex C.9 to resume the call	
9	←		BYE	The SS releases the call with BYE
10	→		200 OK	The UE sends 200 OK for BYE

Specific Message Contents

BYE (Step 9)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 10)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

15.12.5 Test requirements

SS must check that the UE correctly responds to all the mid-dialog INVITEs sent by the SS.

15.12a MT Video Call Hold without announcement

15.12a.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated call hold and resume. This process is described in 3GPP TS 24.610 [108].

15.12a.2 Conformance requirement

[TS 24.610 clause 4.5.2.9]:

Basic communication procedures according to TS 24.229 shall apply.

[TS 24.229 clause 6.1.1]:

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in or 3GPP 29.213.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent; therefore, the RR bandwidth modifier will typically get the value of zero.

[TS 26.114 clause 7.3.1]:

RTCP packets should be sent for all types of multimedia sessions to enable synchronization with other RTP transported media, remote end-point aliveness information, monitoring of the transmission quality, and carriage of feedback messages such as TMMBR for video and RTCP APP for speech. Point-to-point speech only sessions may not require these functionalities and may therefore turn off RTCP by setting the SDP bandwidth modifiers (RR and RS) to zero. When RTCP is turned off (for point-to-point speech only sessions) and the media is put on hold, the MTSI client should re-negotiate the RTCP bandwidth with SDP bandwidth modifiers values greater than zero, and send RTCP packets to the other end. This allows the remote end to detect link aliveness during hold. When media is resumed, the resuming MTSI client should turn off the RTCP sending again through a re-negotiation of the RTCP bandwidth with SDP bandwidth modifiers equal to zero.

Reference(s)

3GPP TS 24.610 [108], TS 24.229 [10]

15.12a.3 Test purpose

1) To verify that the held UE responds correctly to call hold and resume requests from SS.

15.12a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO video call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.8.3-1, steps 1 to 15 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO video call.

Test procedure

1) SS initiates the call hold by sending a re-INVITE to set the media streams into sendonly state.
2) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.
3) SS waits for the UE to respond to the INVITE request with valid 200 OK response.
4) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE.
5) SS resumes the call by sending another re-INVITE request with a SDP offer to set the media streams into sendrecv state again.
6) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.
7) SS waits for the UE to respond to the INVITE request with valid 200 OK response.
8) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE.
9) SS sends a BYE request to the UE in order to release the call.
10) UE responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	**SS**		
1-4			Steps 1-4 specified in annex C.9 to hold the call	
5-8			Steps 1-4 specified in annex C.9 to resume the call	
9	←		BYE	The SS releases the call with BYE
10	→		200 OK	The UE sends 200 OK for BYE

Specific Message Contents

BYE (Step 9)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 10)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

15.12a.5 Test requirements

SS must check that the UE correctly responds to all the mid-dialog INVITEs sent by the SS.

15.13 Incoming Communication Barring except for a specific user

15.13.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Barring (CB) correctly when incoming calls are allowed from one single address only. This process is described in 3GPP TS 24.611 [101].

15.13.2 Conformance requirement

Generic requirements for activating and deactivating Communication Barring can be found from Annexes F.1 and F.5 of this document. Summary of the XML conditions specific to this test case is given here:

[TS 24.611]:

cp:identity: This condition evaluates to true when the remote user's identity matches with the value of the identity element. The interpretation of all the elements of this condition is described in the in the common policy draft (see RFC 4745). In all other cases the condition evaluates to false.

...

ocp:other-identity: If present in any rule, the "other-identity" element, which is empty, matches all identities that are not referenced in any rule. It allows for specifying a default policy. The exact interpretation of this condition is specified in OMA-TS-XDM_Core.

Reference(s)

3GPP TS 24.611 [101].

15.13.3 Test purpose

1) To verify that the UE can request activation of Incoming Communication Barring with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Incoming Communication Barring; and

3) To verify that the UE supporting HTTP Digest authentication can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.13.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Communication Barring;

At step 5b, SS delivers a simservs document as specified in TS 24.611 [101] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <incoming-communication-barring active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
        <cp:conditions>
                   <cp:identity>
                       <cp:many>
                           <cp:except id= px_XCAP_TargetUri>
                           <rule-deactivated/>
                       </cp:many>
                   </cp:identity>
               </cp:conditions>
               <cp:actions>
                   <allow>false</allow>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </incoming-communication-barring>
</simservs>
```

At step 7 deactivation of Communication Barring is respectively triggered at the UE.

15.13.5 Test requirements

1. SS shall check that the UE can authenticate itself with correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

Option 1:

- <incoming-communication-barring> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element for incoming communications barring as follows:
    - <cp:conditions> element containing an <cp:identity> element containing a <cp:many> element
      - element <cp:except id= px_XCAP_TargetUri > within the <cp:many> element and not containing a <rule-deactivated> element
    - <cp:actions> element containing <allow> element with value "false"

Option 2:

- <incoming-communication-barring> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> two rules as follows:
    - one <cp:rule> element for incoming communications barring as follows:
      - <cp:conditions> element containing an <cp:identity> element
        - element <cp:one id= px_XCAP_TargetUri > within the <cp:identity> element and not containing a <rule-deactivated> element
      - <cp:actions> element containing <allow> element with value "true"
    - another <cp:rule> element for incoming communications barring as follows:
      - <cp:conditions> element containing an empty <ocp:other-identity> element and not containing a <rule-deactivated> element
      - <cp:actions> element containing <allow> element with value "false"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> element with "active" attribute being set "false"

or

- <incoming-communication-barring> element with "active" attribute being set "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element found at step 2 for Incoming Communication Barring as follows:
    - <cp:conditions> element containing a <rule-deactivated> element

15.14 Incoming Communication Barring for anonymous users

15.14.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Barring (CB) correctly when incoming calls are rejected for anonymous users. This process is described in 3GPP TS 24.611 [101].

15.14.2 Conformance requirement

Generic requirements for activating and deactivating Communication Barring can be found from Annexes F.1 and F.5 of this document. Summary of the XML conditions specific to this test case is given here:

[TS 24.611, clause 4.2.1]:

The Anonymous Communication Rejection (ACR) service allows the served user to reject incoming communications on which the asserted public user identity of the originating user is restricted. In case the asserted public user identity of the originating user is not provided then the communication shall be allowed by the ACR service.

An example where the originating user restricts presentation of the asserted public user identity is when he activated the OIR service 3GPP TS 24.607.

The originating user is given an appropriate indication that the communication has been rejected due to the application of the ACR service.

The Anonymous Communication Rejection (ACR) simulation service is a special case of the ICB service, which is highlighted here because it is a regulatory service in many countries. The ACR service can be activated for a specific subscriber by configuring an ICB service barring rule where the conditional part contains the "Condition=anonymous" and the action part "allow=false".

[TS 24.611, clause 4.5.2.6.2]:

The AS providing the ACR service shall reject all incoming communications where the incoming SIP request:

1) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "id" as specified in RFC 3325; or

2) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "header" as specified in RFC 3323; or

3) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "user" as specified in RFC 3323; or

4) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "critical" as specified in RFC 3323.

[TS 24.611, clause 4.9.1.4]:

anonymous: To comply with the requirements as set for simulation of the ACR service, the *anonymous* element shall only evaluate to true when the conditions as set out in clause 4.5.2.6.2 for asserted originating public user identity apply.

Reference(s)

3GPP TS 24.611 [101], clauses 4.2.1, 4.5.2.6.2 and 4.9.1.4

15.14.3 Test purpose

1) To verify that the UE can request activation of Anonymous Communication Rejection with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Anonymous Communication Rejection; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.14.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Incoming Communication Barring;

At step 5b, SS delivers a simservs document as specified in TS 24.611 [101] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <incoming-communication-barring active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
        <cp:conditions>
                   <anonymous/>
                   <rule-deactivated/>

               </cp:conditions>
               <cp:actions>
                   <allow>false</allow>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </incoming-communication-barring>
</simservs>
```

At step 7 deactivation of Incoming Communication Barring is respectively triggered at the UE.

15.14.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> element with "active" attribute set as "true" or with “active” attribute not present.

  - within <cp:ruleset> one <cp:rule> element for incoming communications barring as follows:

    - <cp:conditions> element containing an <anonymous> element and not containing a <rule-deactivated> element

    - <cp:actions> element containing <allow> element with value "false"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> element with "active" attribute being set "false"

or

- <incoming-communication-barring> element with "active" attribute set as "true" or with “active” attribute not present.

  - within <cp:ruleset> one <cp:rule> element found at step2 for Incoming Communication Barring as follows:

- <cp:conditions> element containing a <rule-deactivated> element

15.14a Incoming Communication Barring while roaming

15.14a.1 Definition

Test to verify that the UE activates and deactivates the "IMS Multimedia Telephony Communication Barring for incoming calls while the user is roaming" supplementary service while camping on HPLMN. This process is described in 3GPP TS 24.611 [101].

15.14a.2 Conformance requirement

Generic requirements for Communication Barring can be found from Annexes F.1 and F.5.

[TS 24.611, clause 4.9.1.4]:

roaming: This condition evaluates to true when the served user is registered from an access network other then the served users home network.

NOTE: Whether the served user is registered from another network then the served users home network can be determined from the P-Visited-Network-ID header field specified in IETF RFC 3455 and the P-Access-Network-Info header field specified in IETF RFC 3455 both are provided during the registration process, see 3GPP TS 24.229, subclause 5.7.1.3.

Reference(s)

3GPP TS 24.611 [101]

15.14a.3 Test purpose

1) To verify that the UE can request activation of "Communication Barring for incoming calls while the user is roaming" while camping on HPLMN with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Barring; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.14a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Incoming Communication Barring

At step 5b, SS delivers a simservs document as specified in TS 24.611 [101] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <incoming-communication-barring active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
               <cp:conditions>
                    <roaming/>
                    <rule-deactivated/>
               </cp:conditions>
               <cp:actions>
                   <allow>false</allow>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </incoming-communication-barring>
</simservs>
```

At step 7 deactivation of Incoming Communication Barring is respectively triggered at the UE.

15.14a.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element containing a <roaming> element and not containing a <rule-deactivated> element
    - <cp:actions> element containing <allow> element with value "false"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> elements with "active" attribute being set "false" or this element simply deleted

or

- <incoming-communication-barring> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element found at step 2 for incoming communication barring as follows:
    - <cp:conditions> element containing a <rule-deactivated> element

15.14b Outgoing communication Barring while roaming

15.14b.1 Definition

Test to verify that the UE activates and deactivates the "IMS Multimedia Telephony Communication Barring for outgoing calls while the user is roaming" supplementary service while camping on HPLMN. This process is described in 3GPP TS 24.611 [101].

15.14b.2 Conformance requirement

Generic requirements for Communication Barring can be found from Annexes F.1 and F.5.

[TS 24.611, clause 4.9.1.4]:

roaming: This condition evaluates to true when the served user is registered from an access network other then the served users home network.

NOTE: Whether the served user is registered from another network then the served users home network can be determined from the P-Visited-Network-ID header field specified in IETF RFC 3455 and the P-Access-Network-Info header field specified in IETF RFC 3455 both are provided during the registration process, see 3GPP TS 24.229, subclause 5.7.1.3.

Reference(s)

3GPP TS 24.611 [101]

15.14b.3 Test purpose

1) To verify that the UE can request activation of "Communication Barring for outgoing calls while the user is roaming" while camping on HPLMN with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Barring; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.14b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied:

At step 1 activation of Outgoing Communication Barring;

At step 5b, SS delivers a simservs document as specified in TS 24.611 [101] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <outgoing-communication-barring active="true">
         <cp:ruleset>
            <cp:rule id="rule1">
        <cp:conditions>
                  <roaming/>
                  <rule-deactivated/>
               </cp:conditions>
               <cp:actions>
                  <allow>false</allow>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </outgoing-communication-barring>
</simservs>
```

At step 7 deactivation of Outgoing Communication Barring is respectively triggered at the UE.

15.14b.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1) or
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <outgoing-communication-barring> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element containing a <roaming> element and not containing a <rule-deactivated> element
      - <cp:actions> element containing <allow> element with value "false"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <outgoing-communication-barring> elements with "active" attribute being set "false" or this element simply deleted

or

- <outgoing-communication-barring> element with "active" attribute set as "true" or with “active” attribute not present.
  - within <cp:ruleset> one <cp:rule> element found at step 2 for outgoing communication barring as follows:
    - <cp:conditions> element containing a <rule-deactivated> element

15.15 Subscription to the MWI event package

15.15.1 Definition

Test to verify that the UE is able to subscribe to MTSI message waiting notification and handle such notifications received after subscription. This process is described in 3GPP TS 24.229 [10] and TS 24.606 [107].

15.15.2 Conformance requirement

[TS 24.606, clause 4.1]:

The Message Waiting Indication (MWI) service enables the network, upon the request of a controlling user to indicate to the receiving user, that there is at least one message waiting.

[TS 24.606, clause 4.6]:

The application/simple-message-summary MIME type used to provide Message Summary and Message Waiting Indication Information shall be coded as described in clause 5 of RFC 3842.

The coding of the message types in the message-context-class values shall follow the rules defined in the specifications listed in the "reference" column of table 1.

Table 1: Coding requirements

Value	Reference
voice-message	RFC 3458
video-message	RFC 3938
fax-message	RFC 3458
pager-message	RFC 3458
multimedia-message	RFC 3458
text-message	RFC 3458
none	RFC 3458

The coding of the additional information about deposited messages in the application/simple-message-summary MIME type body shall be in alignment with the rules defined in clause 25 of RFC 3261 for SIP extension-header (clause 3.5 of RFC 3842) and follow the rules defined in the specifications listed in the "reference" column of table 2.

Table 2: Additional information

Header	Description	Reference
To:	Indicates the subscriber's public user identity used by correspondent to deposit a message.	clause 3.6.3 of RFC 2822
From:	Indicates the correspondent's public user identity, if available.	clause 3.6.2 of RFC 2822
Subject:	Indicates the topic of the deposited message as provided by correspondent.	clause 3.6.5 of RFC 2822
Date:	Indicates the time and date information about message deposit.	clause 3.6.1 of RFC 2822
Priority:	Indicates the message priority as provided by correspondent.	RFC 2156
Message-ID:	Indicates a single unique message identity.	clause 3.6.4 of RFC 2822
Message-Context:	Indicates a type or context of message.	RFC 3458

[TS 24.606, clause 4.7.1]:

The MWI service is immediately activated after successful SUBSCRIBE request from the subscriber's UE, see clause 4.7.2.

The MWI service is deactivated after subscription expiry or after unsuccessful attempt to deliver a notification about message waiting.

[TS 24.606, clause 4.7.2.1]:

When the subscriber user agent intends to subscribe for status information changes of a message account, it shall generate a SUBSCRIBE request in accordance with RFC 3265 and RFC 3842 and in alignment with the procedures described in TS 24.229.

Depending on the service provisioning the UE will address the SUBSCRIBE request either to one of the subscriber's public user identities or to the public service identity of the message account (see clause 4.5.1).

The subscriber's UE shall implement the "application/simple-message-summary" content type as described in RFC 3842.

Reference(s)

3GPP TS 24.606 clause 4.1, 4.6, 4.7.1 and 4.7.2.1

15.15.3 Test purpose

1) To verify that when subscribing the message waiting indicator the MTSI UE performs correct exchange of SIP protocol signalling messages; and

2) After the receipt of a NOTIFY message for the Message Waiting Indication, if the UE has a UI with the capability to notify the user of a Message Waiting Indication, the UE shall provide the appropriate user indication (which is to be described by the manufacturer) for the message waiting indication.

15.15.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context/EPS bearer, discovered P-CSCF and registered to IMS services, by executing steps 1 to 7 of the generic test procedure in Annex C.2 or steps 1 to 5 of C.2a (GIBA only). The UE is pre-configured to autonomously subscribe to the Message Waiting Indication package. The UE is configured with the public service identity of the message account. Otherwise the phone is expected to use the public identity of the user when subscribing to the Message Waiting Indication package.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE (IMS security) and accepted the registration.

Test procedure

1) The UE sends a SUBSCRIBE request for Message Waiting Indication event package

2) SS responds to the SUBSCRIBE request with a valid 200 OK response

3) SS sends UE a NOTIFY request for the subscribed Message Waiting Indication event package referring to no messages waiting.

4) SS waits for the UE to respond the NOTIFY with a valid 200 OK response.

5) SS sends UE a NOTIFY request for the subscribed Message Waiting Indication event package containing one messages waiting.

6) SS waits for the UE to respond the NOTIFY with a valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		SUBSCRIBE	UE subscribes to the Message Waiting Indication event package.
2	←		200 OK	The SS responds SUBSCRIBE with 200 OK
2a	→		SUBSCRIBE	The UE subscribes to the registration event package
2b	←		200 OK	The SS responds with 200 OK
3	←		NOTIFY	The SS sends initial NOTIFY for Message Waiting Indication event package
4	→		200 OK	The UE responds the NOTIFY with 200 OK
5	←		NOTIFY	The SS sends another NOTIFY for Message Waiting Indication event package, now referring to one voice message waiting
6	→		200 OK	The UE responds the NOTIFY with 200 OK
7	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
8	→		200 OK	The UE responds with 200 OK.

NOTE 1: The default messages contents in annex A are used with condition “IMS security “ or “GIBA” when applicable.

NOTE 2: The SUBSCRIBE messages of step 1 and 2a may occur in any order. Also, the SS can send a 200 OK response as soon as the corresponding SUBSCRIBE message arrived.

Specific Message Contents

SUBSCRIBE (Step 1)

Use the default message “SUBSCRIBE for Message Waiting Indication package” in annex A.6.1

200 OK for SUBSCRIBE (Step 2)

Use the default message “200 OK for SUBSCRIBE” in annex A.1.5

SUBSCRIBE (Step 2a)

Use the default message "SUBSCRIBE for reg-event package" in annex A.1.4

200 OK for SUBSCRIBE (Step 2b)

Use the default message "200 OK for SUBSCRIBE" in annex A.1.5

NOTIFY (Step 3)

Use the default message “NOTIFY for Message Waiting Indication package” in annex A.6.2

200 OK for NOTIFY (Step 4)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

NOTIFY (Step 5)

Use the default message “NOTIFY for Message Waiting Indication package” in annex A.6.2 but with the following exceptions:

Header/param	Value/remark
Message-body	*Messages-Waiting: yes* *Message-Account:* same IMPU as in From header *Voice-Message: 1/0 (0/0)* *To:* <same IMPU as sent by the UE in the From header of the SUBSCRIBE in step 1> *From: <user2_public1@home1.net>* *Subject: call me back!* *Date: Fri 09 Dec 2016 09:15 +0100* *Priority: urgent* *Message-ID: 27775334485*@home domain name *Message-Context: voice-message*

200 OK for NOTIFY (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1

NOTIFY (Step 7)

Use the default message "NOTIFY for reg-event package" in annex A.1.6

200 OK for NOTIFY (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1

15.15.5 Test requirements

The UE shall send requests and responses as described in clause 15.15.4

After step 5, if the UE has a UI with the capability to notify the user of a Message Waiting Indication, it shall indicate to the user the message waiting as per "Description of the user indication for the message waiting".

15.16 Void

15.17 Creating and leaving a conference

15.17.1 Definition

Test to verify that the UE is able to create an IMS MTSI voice conference to the conference focus using conference factory URI. This process is described in 3GPP TS 24.229 [10], TS 24.173 [65] and TS 24.147 [84].

15.17.2 Conformance requirement

[TS 24.147, clause 5.3.1.3]:

A conference can be created by means of SIP, as described in subclause 5.3.1.3.2 or subclause 5.3.1.3.3.

NOTE: Additionally, creation of a conference can be provided by other means.

The conference participant shall make use of the procedures for session establishment as described in subclauses 5.1.2A and 5.1.3 of 3GPP TS 24.229 when creating conferences by means of SIP.

...

Upon a request to create a conference with a conference factory URI, the conference participant shall:

1) generate an initial INVITE request in accordance with subclause 5.1.3.1 of 3GPP TS 24.229; and

2) set the request URI of the INVITE request to the conference factory URI.

On receiving a 200 (OK) response to the INVITE request with the "isfocus" feature parameter indicated in Contact header, the conference participant shall store the content of the received Contact header as the conference URI. In addition to this, the conference participant may subscribe to the conference event package as described in RFC 4575 by using the stored conference URI.

NOTE 1: A conference participant can decide not to subscribe to the conference event package for conferences with a large number of attendees, due to, e.g. the signalling traffic caused by the notifications about users joining or leaving the conference.

NOTE 2: A conference can also be created with a conference URI. The procedures for this case at the conference participant are identical to those for joining a conference, as described in subclause 5.3.1.4.1. It is not assumed that the conference participant is aware that the conference gets created in this case.

NOTE 3: The UE can discover the conference factory URI from the Management Object as defined in 3GPP TS 24.166. Further discovery mechanisms for the conference factory URI are outside the scope of the present document.

...

GIBA:

NOTE 1: GIBA does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A and 5.1.3, TS 24.173 [65], Annex G and TS 24.147 [84], clause 5.3.1.3.

15.17.3 Test purpose

1) To verify that when creating a conference with conference factory URI the UE performs correct exchange of SIP protocol signalling messages with the conference factory; and

2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1).

3) To verify the correct SIP message exchange if the UE optionally subscribes to the conference event package.

15.17.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

1-13) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to14)

13A) UE is triggered to leave the conference.

14) UE leaves the created conference. SS waits the UE to send a BYE request.

15) SS responds to the BYE request with valid 200 OK response.

16) SS notifies the UE that its subscription to conf event is terminated.

17) UE responds with 200 OK.

Expected sequence

Step	Direction UE	Direction SS	Message	Comment
1-13			Steps defined in annex C.10	MTSI conference call created
13A				Make UE leave the conference
14	→		BYE	The UE leaves the conference with BYE
15	←		200 OK	The SS sends 200 OK for BYE
16	←		NOTIFY	If the UE had subscribed to the conference event package, the SS notifies the UE that its subscription to conference event package is terminated
17	→		200 OK	The UE sends 200 OK for NOTIFY (if sent by SS)

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable

Specific Message Contents

Specific Message contents for Steps 1 - 13 as specified in annex C.10

BYE (Step 14)

Use the default message “BYE” in annex A.2.8 but with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName

200 OK for BYE (Step 15)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

NOTIFY (Step 16)

Use the default message “NOTIFY for conference event package” in annex A.5.3 with condition A4.

200 OK for NOTIFY (Step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

15.17.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.18 Inviting user to conference by sending a REFER request to the user

15.18.1 Definition

Test to verify that the UE is able to invite an user to a conference by sending a REFER request directly to the invited user. This process is described in 3GPP TS 24.147 [84].

15.18.2 Conformance requirement

[TS 24.147, clause 5.3.1.5.2]:

Upon generating a REFER request that is destined to a user in order to invite that user to a specific conference, the conference participant shall:

1) set the request URI of the REFER request to the address of the user who is invited to the conference;

2) set the Refer-To header of the REFER request to the conference URI of the conference that the other user shall be invited to, including the "method" URI parameter set to "INVITE" or omit the "method" parameter; and

NOTE: Other headers of the REFER request will be set in accordance with 3GPP TS 24.229

3) send the REFER request towards the user who is invited to the conference.

The UE may additionally include the Referred-By header to the REFER request and set it to the URI of the conference participant that is sending the REFER request.

Afterwards the UE shall treat incoming NOTIFY requests that are related to the previously sent REFER request in accordance with RFC 3515 and may indicate the received information to the user.

Reference(s)

3GPP TS 24.147[84], clause 5.3.1.5.2

15.18.3 Test purpose

1) To verify that the UE sends a correctly composed REFER request to invite a user to conference; and

2) To verify that the UE correctly processes the NOTIFYs from the invited user; and

3) To verify that the UE correctly processes the NOTIFYs for the conference event package if the UE has subscribed to those.

15.18.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, registered to IMS services by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter created a conference by executing the generic test procedure in Annex C.10 up to its last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and conference.

Test procedure

1) UE invites a user to the conference created. SS waits the UE to send to the invited user a REFER request, which refers to the conference created.

2) SS responds to the REFER request with a valid 202 Accepted response.

3) SS sends an initial NOTIFY to tell that the invited user is trying to join the conference.

4) UE responds to the NOTIFY request with valid 200 OK response.

5) SS sends the final NOTIFY to tell that the invited user has successfully joined the conference.

6) UE responds to the NOTIFY request with a valid 200 OK response.

7) Optional: If UE subscribed the conference event package during the generic test procedure of Annex C.10, SS sends a NOTIFY for the conference event package to the UE to notify that the user joined the conference.

8) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REFER	UE sends REFER to SS referring to the conference
2	←		202 Accepted	The SS responds with a 202 final response
3	←		NOTIFY	The SS sends initial NOTIFY for the implicit subscription created by the REFER request
4	→		200 OK	The UE responds the NOTIFY with 200 OK
5	←		NOTIFY	The SS sends a NOTIFY related to REFER request to confirm that the invited user was able to join the conference
6	→		200 OK	The UE responds the NOTIFY with 200 OK
7	←		NOTIFY	Optional: If the UE has subscribed the conference event package, the SS sends a NOTIFY for conference event package to inform that the invited user was able to join the conference
8	→		200 OK	Optional: The UE responds the NOTIFY with 200 OK

Specific Message Contents

REFER (Step 1)

Use the default message "MO REFER" in annex A.2.10 with the following exceptions:

Header/param	Value/remark
Request-URI	SIP URI of the user invited to the conference
Refer-To	
addr-spec	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
To	
addr-spec	SIP URI of the user invited to the conference
tag	no tag given
Call-ID	
callid	value different to that received in INVITE message used to create the conference
CSeq	
value	must be present, value not checked

202 Accepted for REFER (Step 2)

Use the default message "202 Accepted" in annex A.3.3.

NOTIFY (Step 3)

Use the default message "MT NOTIFY for refer package" in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

NOTIFY (Step 5)

Use the default message "MT NOTIFY for refer package" in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

200 OK for NOTIFY (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

NOTIFY (Step 7)

Use the default message "NOTIFY for conference event package" in annex A.5.3 with the following exceptions:

Header/param	Value/remark
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<conference-info xmlns="urn:ietf:params:xml:ns:conference-info">* *entity="sip:final@conf-factory.* appended with px_IMS_HomeDomainName*"* *state="partial"* *version="1"* *<users>* *<user entity="* **SIP URI of the invited user***">* *<endpoint entity="* **Contact URI of the invited user***">* *<status>connected</status>* *<joining-method>dialed-in</joining-method>* *<media id="1">* *<type>audio</type>* *<label>11223</label>* *<src-id>***random SSRC value***</src-id>* *<status>sendrecv</status>* *</media>* *</endpoint>* *</users>* *</conference-info>*

200 OK for NOTIFY (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

15.18.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.19 Inviting user to conference by sending a REFER request to the conference focus

15.19.1 Definition

Test to verify that the UE is able to invite a user to an audio conference by sending a REFER request to the conference focus. This process is described in 3GPP TS 24.147 [84].

15.19.2 Conformance requirement

[TS 24.147, clause 5.3.1.5.3]:

Upon generating a REFER request in accordance with the procedures specified in 3GPP TS 24.229, IETF RFC 3515 as updated by IETF RFC 6665 and IETF RFC 7647 that is destined to the conference focus in order to invite another user to a specific conference, the conference participant shall:

1) set the request URI of the REFER request to the conference URI to which the user is invited to;

2) set the Refer-To header of the REFER request to the SIP URI or tel URL of the user who is invited to the conference;

3) either include the "method" URI parameter with the value "INVITE" or omit the "method" URI parameter in the Refer-To header; and

NOTE: Other headers of the REFER request will be set in accordance with 3GPP TS 24.229.

4) send the REFER request towards the conference focus that is hosting the conference.

The UE may additionally include the Referred-By header to the REFER request and set it to the URI of the conference participant that is sending the REFER request.

In case of an active session the UE may additionally include the Replaces header in the header portion of the SIP URI of the Refer-to header of the REFER request. If the user involved in the active session is identified by a tel URI, the UE shall convert the tel URI to an SIP URI as described in RFC 3261 before including the Replaces header field. The included Replaces header shall refer to the active dialog that is replaced by the ad-hoc conference. The Replaces header shall comply with RFC 3891.

Afterwards the UE shall treat incoming NOTIFY requests that are related to the previously sent REFER request in accordance with RFC 3515 as updated by RFC 6665 and may indicate the received information to the user.

Reference(s)

3GPP TS 24.147 [84], clause 5.3.1.5.3

15.19.3 Test purpose

1) To verify that the UE sends a correctly composed REFER request to invite a user to a conference; and

2) To verify that the UE correctly processes the NOTIFYs from the invited user; and

3) To verify that the UE correctly processes the NOTIFYs for the conference event package if the UE has subscribed to those.

15.19.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services by executing the generic test procedure in Annex C.2 up to the last step and thereafter created a conference by executing the generic test procedure in Annex C.10 up to its last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and conference.

Test procedure

1) UE invites a user to the conference created. SS waits for the UE to send to the conference focus a REFER request, which refers to the user to be invited to the conference.

2-9) UE sends REFER to focus and receives corresponding notifications.

9A) UE is triggered to leave the conference.

10-11) UE leaves conference.

12-13) SS notifies UE about subscription end.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE invite another user to the conference	UE sends REFER to SS referring to the conference
2-9			Steps defined in annex C.19	
9A				Make UE leave the conference
10	→		BYE	The UE leaves the conference with BYE
11	←		200 OK	The SS sends 200 OK for BYE
12	←		NOTIFY	If the UE had subscribed to the conference event package, the SS notifies the UE that its subscription to conference event package is terminated
13	→		200 OK	The UE sends 200 OK for NOTIFY (if sent by SS)

Specific Message Contents

BYE (Step 10)

Use the default message "BYE" in annex A.2.8 but with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName

200 OK for BYE (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

NOTIFY (Step 12)

Use the default message "NOTIFY for conference event package" in annex A.5.3 with condition A4.

200 OK for NOTIFY (Step 13)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

15.19.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.19a Inviting user to conference by sending a REFER request to the conference focus / Video

15.19a.1 Definition

Test to verify that the UE is able to invite a user to a video conference by sending a REFER request to the conference focus. This process is described in 3GPP TS 24.147 [84].

15.19a.2 Conformance requirement

[TS 24.147, clause 5.3.1.5.3]:

Upon generating a REFER request in accordance with the procedures specified in 3GPP TS 24.229, IETF RFC 3515 as updated by IETF RFC 6665 and IETF RFC 7647 that is destined to the conference focus in order to invite another user to a specific conference, the conference participant shall:

1) set the request URI of the REFER request to the conference URI to which the user is invited to;

2) set the Refer-To header of the REFER request to the SIP URI or tel URL of the user who is invited to the conference;

3) either include the "method" URI parameter with the value "INVITE" or omit the "method" URI parameter in the Refer-To header; and

NOTE: Other headers of the REFER request will be set in accordance with 3GPP TS 24.229.

4) send the REFER request towards the conference focus that is hosting the conference.

The UE may additionally include the Referred-By header to the REFER request and set it to the URI of the conference participant that is sending the REFER request.

In case of an active session the UE may additionally include the Replaces header in the header portion of the SIP URI of the Refer-to header of the REFER request. If the user involved in the active session is identified by a tel URI, the UE shall convert the tel URI to an SIP URI as described in RFC 3261 before including the Replaces header field. The included Replaces header shall refer to the active dialog that is replaced by the ad-hoc conference. The Replaces header shall comply with RFC 3891.

Afterwards the UE shall treat incoming NOTIFY requests that are related to the previously sent REFER request in accordance with RFC 3515 as updated by RFC 6665 and may indicate the received information to the user.

Reference(s)

3GPP TS 24.147 [84], clause 5.3.1.5.3

15.19a.3 Test purpose

1) To verify that the UE sends a correctly composed REFER request to invite a user to a conference; and

2) To verify that the UE correctly processes the NOTIFYs from the invited user; and

3) To verify that the UE correctly processes the NOTIFYs for the conference event package if the UE has subscribed to those.

15.19a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services by executing the generic test procedure in Annex C.2 up to the last step and thereafter created a conference by executing the generic test procedure in Annex C.38 up to its last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and conference.

Test procedure

1) UE invites a user to the conference created. SS waits for the UE to send to the conference focus a REFER request, which refers to the user to be invited to the conference.

2) SS responds to the REFER request with a valid 202 Accepted response.

3) SS sends an initial NOTIFY to tell that the invited user is trying to join the conference.

4) UE responds to the NOTIFY request with valid 200 OK response.

5) SS sends the final NOTIFY request to tell that the invited user has successfully joined the conference.

6) UE responds to the NOTIFY request with a valid 200 OK response.

7) Optional: If UE subscribed the conference event package during the generic test procedure of Annex C.10, SS sends a NOTIFY request for the conference event package to the UE to notify that the user joined the conference.

8) If SS sent a NOTIFY request, SS waits for the UE to respond to the NOTIFY request with 200 OK response.

9) UE is triggered to leave the conference.

10) UE sends BYE in ordre to leave the conference

11) SS responds with 200 OK

12) SS notifies the UE that its subscription to conf event is terminated.

13) UE responds with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE invite another user to the conference	
2-8a			Steps defined in annex C.19	
9				Make UE leave the conference
10	→		BYE	The UE leaves the conference with BYE
11	←		200 OK	The SS sends 200 OK for BYE
12	←		NOTIFY	If the UE had subscribed to the conference event package, the SS notifies the UE that its subscription to conference event package is terminated
13	→		200 OK	The UE sends 200 OK for NOTIFY (if sent by SS)

Specific Message Contents

BYE (Step 10)

Use the default message "BYE" in annex A.2.8 but with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName

200 OK for BYE (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

NOTIFY (Step 12)

Use the default message "NOTIFY for conference event package" in annex A.5.3 with condition A4.

200 OK for NOTIFY (Step 13)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

15.19a.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.20 Void

15.21 Joining a conference after being invited to it

15.21.1 Definition

Test to verify that the UE is able to join a MTSI voice conference after being invited to it. This process is described in 3GPP TS 24.147 [84].

15.21.2 Conformance requirement

[TS 24.147, clause 5.3.1.4.1]:

Upon generating an initial INVITE request to join a conference for which the conference URI is known to the conference participant, the conference participant shall:

1) set the request URI of the INVITE request to the conference URI; and

2) send the INVITE request towards the conferencing AS that is hosting the conference.

NOTE 1: The initial INVITE request is generated in accordance with 3GPP TS 24.229.

NOTE 2: The conference participants can get the conference URI as described in subclause 5.3.1.4.2. Other mechanisms can also be used by the conference participant to become aware of the conference URI, but they are out of scope of this specification..

On receiving a 200 (OK) response to the INVITE request with the "isfocus" feature parameter indicated in Contact header, the conference participant shall store the contents of the received Contact header as the conference URI. In addition to that, the conference participant may subscribe to the conference event package as described in RFC 4575 by using the stored conference URI.

NOTE 3: A conference participant can decide not to subscribe to the conference event package for conferences with a large number of attendees, due to the signalling traffic caused by the notifications about e.g. users joining or leaving the conference.

Upon receipt of an INVITE request that includes a Replaces header, the conference participant shall apply the procedures described in RFC 3891 to the INVITE request.

[TS 24.147, clause 5.3.1.4.2]:

Upon receipt of a REFER request that either includes a Refer-To header which includes the "method" uri parameter set to INVITE or does not include the "method" URI parameter, the conference participant shall:

1) handle the REFER request in accordance with RFC 3515;
2) perform the actions as described in subclause 5.3.1.4.1 for a user joining a conference; and
3) if the received REFER request included a Referred-By header, include the Referred-By header in accordance with RFC 3892 in the INVITE request that is sent for joining the conference.

Reference(s)

3GPP TS 24.147 [84], clauses 5.3.1.4.1 and 5.3.1.4.2

15.21.3 Test purpose

1) To verify that the UE correctly processes the REFER request which invites the user to join the conference; and
2) To verify that the UE issues correctly composed NOTIFYs to report its progress; and
3) To verify that the UE sets up a new dialog with conference focus by sending an INVITE request; and
4) To verify that the UE terminates the dialog with the conference focus when receiving a BYE request.

15.21.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

0) SS pages the UE to perform procedure described in TS 36.508 [94] table 4.5A.7.3-1 steps 1-8
1) SS sends to the UE a REFER request, which refers to the conference focus.
2) SS waits the UE to respond to the REFER request with a valid 202 Accepted response.
3) SS waits the UE to send an INVITE request to the conference focus
4) SS responds to the INVITE request with a 100 Trying response
5) SS waits the UE to send an initial NOTIFY to tell that it is trying to join the conference.
6) SS responds to the NOTIFY request with valid 200 OK response.
7) SS responds to the INVITE request with a 183 Session in Progress response

7a) SS starts activation of dedicated EPS bearer according to TS 36.508 [94] table 4.5A.7.3-1 steps 13-15

8) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

9) SS responds to the PRACK request with valid 200 OK response.

10) SS waits for the UE to optionally send a UPDATE request containing the final SDP offer. UE will not send the UPDATE request if the PRACK in step 8 already contained the final offer with preconditions met.

11) SS responds to the UPDATE request (if UE sent one) with valid 200 OK response.

12) SS responds to the INVITE request with a 200 OK response

13) SS waits the UE to send an ACK and NOTIFY requests. Additionally the UE may send a SUBCRIBE request for the conference event package. The UE is allowed to send these requests in any order.

14) SS responds to the NOTIFY request with a valid 200 OK response.

15) If UE sent SUBSCRIBE, SS responds to it with 200 OK response.

16) If UE sent SUBSCRIBE, SS sends a NOTIFY for the conference event package to the UE.

17) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

18) SS sends a BYE request in order to remove the UE from the conference

19) SS waits the UE to respond to the BYE request with a valid 200 OK response.

20) SS notifies the UE that its subscription to conf event is terminated.

21) UE responds with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
0				Radio Bearer Establishment according to TS 36.508 [94] table 4.5A.7.3-1 (steps 1 to 8)
1	←		REFER	SS sends REFER to UE referring to the conference
2	→		202 Accepted	UE responds with a 202 Accepted response
3	→		INVITE	UE sends INVITE to set up a dialog with conference focus. UE indicates the medias and codecs the UE supports.
4	←		100 Trying	SS responds the INVITE with 100 Trying
5	→		NOTIFY	UE sends initial NOTIFY for the implicit subscription created by the REFER request
6	←		200 OK	SS responds the NOTIFY with 200 OK
7	←		183 Session in Progress	SS responds with an SDP answer only supporting AMR audio codec
7a				Activation of dedicated EPS bearer according to TS 36.508 [94] table 4.5A.7.3-1 steps 13-15 NOTE: Activation is started by the SS but messages sent by the UE are in parallel to step 8
8	→		PRACK	UE acknowledges the receipt of 183 response with PRACK and optionally offers second SDP that indicates preconditions as met
9	←		200 OK	The SS responds PRACK with 200 OK and answers the second SDP with mirroring its contents and indicates having reserved the resources if UE has also done so.
10	→		UPDATE	Optional step: UE sends an UPDATE after having reserved the resources with GPRS procedures for PDP context used for the media
11	←		200 OK	Optional step: The SS responds UPDATE with 200 OK and indicates having reserved the resources
12	←		200 OK	SS responds the INVITE with 200 OK
13	→		ACK NOTIFY SUBSCRIBE (optional message)	UE sends the ACK to complete three-way handshake for INVITE and NOTIFY to confirm that the UE was able to join the conference. Additionally the UE may subscribe to the conference event package related to the conference to which the user joined. Note that the UE may send these messages in any order; the SS shall wait up to 3s for the UE to send the optional SUBSCRIBE
14	←		200 OK	SS responds the NOTIFY with 200 OK
15	←		200 OK	Optional step: SS responds to the subscription if the UE sent the SUBSCRIBE request
16	←		NOTIFY	Optional step: SS sends the initial state of the conference event to the UE if the UE subscribed it
17	→		200 OK	Optional step: UE responds to the NOTIFY
18	←		BYE	SS sends a BYE to remove the UE from the conference
19	→		200 OK	UE responds the BYE with 200 OK
20	←		NOTIFY	If the UE had subscribed to the conference event package, the SS notifies the UE that its subscription to conference event package is terminated
21	→		200 OK	The UE sends 200 OK for NOTIFY (if sent by SS)

In addition to the steps shown above the UE might send extra NOTIFY requests to indicate the progress e.g. after receiving the 183 response from the SS. As the timing of these optional NOTIFY requests from the UE is not deterministic, they are not shown in the expected sequence. SS must be prepared to receive such NOTIFY requests between steps 3 and 13 and respond to them with 200 OK response.

Specific Message Contents

REFER (Step 1)

Use the default message "MT REFER" in annex A.2.12 with the following exceptions:

Header/param	Value/remark
Request-URI	Contact URI of the UE invited to the conference (as within the REGISTER request from the UE)
Refer-To	
addr-spec	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
Referred-by	-- check this
addr-spec	*sip:master@conference.com*
To	
addr-spec	SIP URI of the user invited to the conference
tag	no tag given
Call-ID	
callid	any value according to Call-ID syntax can be used
CSeq	
value	any value according to CSeq syntax can be used

202 Accepted for REFER (Step 2)

Use the default message "202 Accepted" in annex A.3.3.

INVITE (Step 3)

Use the default message "INVITE for MO call setup" in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
To	
addr-spec	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
Referred-by	
addr-spec	*sip:master@conference.com*
Supported	
option-tag	*precondition*
Message-body	*The following SDP types and values.* *Session description:* - *v=0* - *o=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE)* - *s=(session name)* - *c=IN (addrtype) (connection-address for UE) [Note 1]* - *b=AS: (bandwidth-value)* *Time description:* - *t= (start-time) (stop-time)* *Media description:* - *m=audio (transport port) RTP/AVP (fmt)* - *c=IN (addrtype) (connection-address for UE) [Note 1]* - *b=AS: (bandwidth-value)* - *b=RS: (bandwidth-value)* - *b=RR: (bandwidth-value)* *Attributes for media:* - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:* (format) *mode-change-capability=2; max-red=(att-field)* [Note 3] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=ptime:20* - *a=maxptime:240* *Attributes for preconditions:* - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* *Note 1: At least one "c=" field shall be present.* *Note 2: The AMR channel number shall be "/1" or omitted.* *Note 3: Values from 0 to 220 are allowed*

100 Trying for INVITE (Step 4)

Use the default message "100 Trying for INVITE" in annex A.2.2.

NOTIFY (Step 5)

Use the default message "MO NOTIFY for refer package" in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

183 Session in Progress for INVITE (Step 7)

Use the default message "183 Session in Progress for INVITE" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Require	
option-tag	*precondition*
Contact	
addr-spec	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
Message-body	The following SDP types and values. Session description: - *v=0* - *o=1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) AMR-*WB*/16000/1 [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* - *a=inactive* [Note 2] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, bandwidth, payload type and format copied from step 3. Note 2: The attribute a=inactive shall be present if it was included in step 3.

PRACK (Step 8)

Use the default message “PRACK” in annex A.2.4 with the exception that either Supported or Require header shall contain the "precondition" tag and with the following exceptions:

Header/param	Value/remark
Content-Type media-type	header shall be present only if there is SDP in message-body *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this request and if there is a message-body length of message-body
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one Note 3: The AMR channel number shall be “/1” or omitted.

200 OK for PRACK (Step 9)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	header shall be present only if there is SDP in message-body *application/sdp*
Content-Length value	 length of message-body
Message-body	Header present if Prack (step 8) contained SDP. Contents if present: SDP body of the 200 response copied from the received PRACK and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: *a=curr:qos remote sendrecv*

UPDATE (Step 10) optional step used when PRACK contained a=curr:qos local none

Use the default message "UPDATE" in annex A.2.5 with the exception that either Supported or Require header shall contain the "precondition" tag and with the following exceptions:

Header/param	Value/remark
Message-body	Same contents as specified in step 8.

200 OK for UPDATE (Step 11) - optional step used when UE sent UPDATE

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE but modified as follows: "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - the "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31], updated as follows: a=curr:qos local sendrecv a=curr:qos remote sendrecv a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv

200 OK for INVITE (Step 12)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact addr-spec	 *sip:final@conf-factory.* appended with px_IMS_HomeDomainName

ACK (Step 13)

Use the default message “ACK” in annex A.2.7.

NOTIFY (Step 13)

Use the default message “MO NOTIFY for refer package” in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

SUBSCRIBE (Step 13)

Use the default message “SUBSCRIBE for conference event package” in annex A.5.1.

200 OK for NOTIFY (Step 14)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

200 OK for SUBSCRIBE (Step 15)

Use the default message “200 OK for SUBSCRIBE” in annex A.5.2.

NOTIFY (Step 16)

Use the default message “NOTIFY for conference event package” in annex A.5.3 with condition A3.

200 OK for NOTIFY (Step 17)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

BYE (Step 18)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 19)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

NOTIFY (Step 20)

Use the default message “NOTIFY for conference event package” in annex A.5.3 with condition A4.

200 OK for NOTIFY (Step 21)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

15.21.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 3: the UE shall send an INVITE message with correct content according to the Specific Message Contents above.

Step 8: the UE shall send a PRACK request with the correct content according to the Specific Message Contents above.

Step 10: the UE may conditionally send an UPDATE request with the correct content according to the Specific Message Contents above.

15.21a Three way session creation

15.21a.1 Definition

Test to verify that the UE support Three Way Session creation. This process is described in Section 5.3.1.3.3 of 3GPP TS 24.147 [84].

15.21a.2 Conformance requirement

[TS 24.147 clause 5.3.1.3.3]:

When a user is participating in two or more SIP sessions and wants to join together two of these active sessions to a so-called three-way session, the user shall perform the following steps.

1) create a conference at the conference focus by sending an INVITE request with the conference factory URI for the three-way session towards the conference focus, as described in subclause 5.3.1.3.2;

2) decide and perform for each of the active sessions that are requested to be joined to the three-way session, how the remote user shall be invited to the three-way session, which can either be:

   a) by performing the procedures for inviting a user to a conference by sending an REFER request to the user, as described in subclause 5.3.1.5.2; or

   b) by performing the procedures for inviting a user to a conference by sending a REFER request to the conference focus, as described in subclause 5.3.1.5.3;

3) release the active session with the user, by applying the procedures for session release in accordance with RFC 3261 [7], provided that a BYE request has not already been received, after a NOTIFY request has been received, indicating that the user has successfully joined the three-way session, i.e. including:

   a) a body of content-type "message/sipfrag" that indicates a "200 OK" response; and,

   b) a Subscription-State header set to the value "terminated"; and,

4) treat the created three-way session as a normal conference, i.e. the conference participant shall apply the applicable procedures of subclause 5.3.1 for it.

Reference(s)

3GPP TS 24.147 [84]

15.21a.3 Test purpose

1) To verify that the invoking UE is able to create a three-way session by sending a REFER request to the conference focus to inviting a user to a conference;

15.21a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-4) Call hold is initiated on the UE. The same steps defined in Annex C.8 are used to put the call into hold.

5-17) A new session is created by using the steps defined in Annex C.21.

17A) The UE is triggered to start a multiparty call. This causes the UE to first put the second call on hold as described in Steps 17B-17E, and then to initiate the following steps 19-46D.

17B-17E) The UE puts the second call on hold by executing the steps described in Annex C.8

19-30) UE initiates the conference creation process by executing steps 2-13 of the generic test procedure in Annex C.10.

31-38) UE invites one of the user who have session with the UE to the conference by performing the same procedure as in Annex C.19.

39-46D) UE invites another user who have session with the UE to the conference by performing the same procedure as in Annex C.19.

UE shall send two BYE requests to terminate the two initial calls it put on hold. SS responds to the BYE requests with a valid 200 OK response each.

47) SS sends a BYE request to the UE in order to release the active session if BYE request has not already been received.

48) UE responds to the BYE request with valid 200 OK response.

49) SS notifies the UE that its subscription to conf event is terminated.

50) UE responds with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-4			Messages in Annex C.8	The same messages as in Annex C.8 Steps 1-4 are used to put the first call on hold.
5-17			Steps defined in Annex C.21	The same messages as in Annex C.21 are used to start a second call.
17A				Make UE start a Multiparty Call
17B-17E			Messages in Annex C.8	The same messages as in Annex C.8 Steps 1-4 are used to put the second call on hold
18				Void
19-30			Steps 2-13 defined in Annex C.10	The same messages as in Annex C.10 are used.
31-38			Steps defined in Annex C.19	The same messages as in Annex C.19 steps 1-8 are used.
39-46	→		Steps defined in Annex C.19	The same messages as in Annex C.19 steps 1-8 are used.
46A	→		BYE	UE shall send a BYE to terminate the first call
46B	←		200 OK	The SS responds the received BYE with 200 OK
46C	→		BYE	UE shall send a BYE to terminate the second call.
46D	←		200 OK	The SS responds the received BYE with 200 OK
47	←		BYE	The SS releases the active session with BYE
48	→		200 OK	The UE sends 200 OK for BYE
49	←		NOTIFY	If the UE had subscribed to the conference event package, the SS notifies the UE that its subscription to conference event package is terminated
50	→		200 OK	The UE sends 200 OK for NOTIFY (if sent by SS)

NOTE 1: Steps 27-30 (i.e., steps 10-13 of C.10) are optional. Therefore, UE can start with steps 31-46 right away after Step 26. If Steps 27-30 are executed, they can happen in parallel to Steps 31-46.

NOTE 2: The two executions of Annex C.19, i.e., steps 31-38 and steps 39-46, can run in parallel.

NOTE 3: Step 46A can happen any time after step 35. The SS sends the corresponding 200 OK message right after having received the BYE message.

NOTE 4: Step 46C can happen any time after step 43. The SS sends the corresponding 200 OK message right after having received the BYE message.

Specific Message Contents

INVITE(Step 6)

Use the default message "INVITE" in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	px_IMS_CalleeUri2 px_IMS_CalleeUri2 is used to invite another user to the session. px_IMS_CalleeUri2 may be either SIP or Tel URI. It may contain a dialstring and phone-context parameter, when calling to dialstring. When calling to dialstring SIP URI must also contain user=phone or user=dialstring parameter. The dialstring, if used, may be global, home local number or geo-local number. For home local numbers the value of phone-context parameter must equal the home domain name i.e. px_IMS_HomeDomainName. For geo-local numbers the home domain name must be prefixed by string "geo-local." or access technology specific prefix, if the UE supports that option. Note: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is UE implementation specific. For instance the UE might have a UI setting.
To	
addr-spec	px_IMS_CalleeUri2

183 Session in Progress for INVITE (Step 8)

Use the default message "183 Session in Progress for INVITE" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

180 Ringing for INVITE (Step 13)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

200 OK for INVITE (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

BYE (Step 47)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 48)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

NOTIFY (Step 49)

Use the default message “NOTIFY for conference event package” in annex A.5.3 with condition A4.

200 OK for NOTIFY (Step 50)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

15.21a.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

The UE shall send requests and responses as described in clause 15.21a.4.

15.21b Joining a conference after being invited to it / Video

15.21b.1 Definition

Test to verify that the UE is able to join a MTSI voice conference after being invited to it. This process is described in 3GPP TS 24.147 [84].

15.21b.2 Conformance requirement

[TS 24.147, clause 5.3.1.4.1]:

Upon generating an initial INVITE request to join a conference for which the conference URI is known to the conference participant, the conference participant shall:

1) set the request URI of the INVITE request to the conference URI; and

2) send the INVITE request towards the conferencing AS that is hosting the conference.

NOTE 1: The initial INVITE request is generated in accordance with 3GPP TS 24.229.

NOTE 2: The conference participants can get the conference URI as described in subclause 5.3.1.4.2. Other mechanisms can also be used by the conference participant to become aware of the conference URI, but they are out of scope of this specification.

On receiving a 200 (OK) response to the INVITE request with the "isfocus" feature parameter indicated in Contact header, the conference participant shall store the contents of the received Contact header as the conference URI. In addition to that, the conference participant may subscribe to the conference event package as described in RFC 4575 by using the stored conference URI.

NOTE 3: A conference participant can decide not to subscribe to the conference event package for conferences with a large number of attendees, due to the signalling traffic caused by the notifications about e.g. users joining or leaving the conference.

Upon receipt of an INVITE request that includes a Replaces header, the conference participant shall apply the procedures described in RFC 3891 to the INVITE request.

[TS 24.147, clause 5.3.1.4.2]:

Upon receipt of a REFER request that either includes a Refer-To header which includes the "method" uri parameter set to INVITE or does not include the "method" URI parameter, the conference participant shall:

1) handle the REFER request in accordance with RFC 3515;
2) perform the actions as described in subclause 5.3.1.4.1 for a user joining a conference; and
3) if the received REFER request included a Referred-By header, include the Referred-By header in accordance with RFC 3892 in the INVITE request that is sent for joining the conference.

Reference(s)

3GPP TS 24.147 [84], clauses 5.3.1.4.1 and 5.3.1.4.2

15.21b.3 Test purpose

1) To verify that the UE correctly processes the REFER request which invites the user to join the conference; and
2) To verify that the UE issues correctly composed NOTIFYs to report its progress; and
3) To verify that the UE sets up a new dialog with conference focus by sending an INVITE request; and
4) To verify that the UE terminates the dialog with the conference focus when receiving a BYE request.

15.21b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

0) SS pages the UE to perform procedure described in TS 36.508 [94] table 4.5A.9.3-1 steps 1-8
1) SS sends to the UE a REFER request, which refers to the conference focus.
2) SS waits the UE to respond to the REFER request with a valid 202 Accepted response.
3) SS waits the UE to send an INVITE request to the conference focus
4) SS responds to the INVITE request with a 100 Trying response
5) SS waits the UE to send an initial NOTIFY to tell that it is trying to join the conference.
6) SS responds to the NOTIFY request with valid 200 OK response.
7) SS responds to the INVITE request with a 183 Session in Progress response

7a) SS starts activation of dedicated EPS bearers according to TS 36.508 [94] table 4.5A.9.3-1 steps 13-16

8) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.
9) SS responds to the PRACK request with valid 200 OK response.
10) SS waits for the UE to optionally send a UPDATE request containing the final SDP offer. UE will not send the UPDATE request if the PRACK in step 8 already contained the final offer with preconditions met.

11) SS responds to the UPDATE request (if UE sent one) with valid 200 OK response.

12) SS responds to the INVITE request with a 200 OK response

13) SS waits the UE to send an ACK and NOTIFY requests. Additionally the UE may send a SUBCRIBE request for the conference event package. The UE is allowed to send these requests in any order.

14) SS responds to the NOTIFY request with a valid 200 OK response.

15) If UE sent SUBSCRIBE, SS responds to it with 200 OK response.

16) If UE sent SUBSCRIBE, SS sends a NOTIFY for the conference event package to the UE.

17) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

18) SS sends a BYE request in order to remove the UE from the conference

19) SS waits the UE to respond to the BYE request with a valid 200 OK response.

20) SS notifies the UE that its subscription to conf event is terminated.

21) UE responds with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
0				Radio Bearer Establishment according to TS 36.508 [94] table 4.5A.9.3-1 (steps 1 to 8)
1	←		REFER	SS sends REFER to UE referring to the conference
2	→		202 Accepted	UE responds with a 202 Accepted response
3	→		INVITE	UE sends INVITE to set up a dialog with conference focus. UE indicates the medias and codecs the UE supports.
4	←		100 Trying	SS responds the INVITE with 100 Trying
5	→		NOTIFY	UE sends initial NOTIFY for the implicit subscription created by the REFER request
6	←		200 OK	SS responds the NOTIFY with 200 OK
7	←		183 Session in Progress	SS responds with an SDP answer indicating speech and video.
7a				Activation of dedicated EPS bearers according to TS 36.508 [94] table 4.5A.9.3-1 steps 13-16 NOTE: Activation is started by the SS but messages sent by the UE are in parallel to step 8
8	→		PRACK	UE acknowledges and optionally offer a second SDP if a dedicated EPS bearer is established by the network.
9	←		200 OK	The SS responds PRACK with 200 OK and answers the second SDP with mirroring its contents and indicates having reserved the resources if UE has also done so.
10	→		UPDATE	Optional step: UE sends a second SDP if a dedicated EPS bearer is established by the network.
11	←		200 OK	Optional step: The SS responds UPDATE with 200 OK and indicates having reserved the resources
12	←		200 OK	SS responds the INVITE with 200 OK
13	→		ACK NOTIFY SUBSCRIBE (optional message)	UE sends the ACK to complete three-way handshake for INVITE and NOTIFY to confirm that the UE was able to join the conference. Additionally the UE may subscribe to the conference event package related to the conference to which the user joined. Note that the UE may send these messages in any order; the SS shall wait up to 3s for the UE to send the optional SUBSCRIBE
14	←		200 OK	SS responds the NOTIFY with 200 OK
15	←		200 OK	Optional step: SS responds to the subscription if the UE sent the SUBSCRIBE request
16	←		NOTIFY	Optional step: SS sends the initial state of the conference event to the UE if the UE subscribed it
17	→		200 OK	Optional step: UE responds to the NOTIFY
18	←		BYE	SS sends a BYE to remove the UE from the conference
19	→		200 OK	UE responds the BYE with 200 OK
20	←		NOTIFY	If the UE had subscribed to the conference event package, the SS notifies the UE that its subscription to conference event package is terminated
21	→		200 OK	The UE sends 200 OK for NOTIFY (if sent by SS)

In addition to the steps shown above the UE might send extra NOTIFY requests to indicate the progress e.g. after receiving the 183 response from the SS. As the timing of these optional NOTIFY requests from the UE is not deterministic, they are not shown in the expected sequence. SS must be prepared to receive such NOTIFY requests between steps 3 and 13 and respond to them with 200 OK response.

Specific Message Contents

REFER (Step 1)

Use the default message “MT REFER” in annex A.2.12 with the following exceptions:

Header/param	Value/remark
Request-URI	Contact URI of the UE invited to the conference (as within the REGISTER request from the UE)
Refer-To addr-spec	 *sip:final@conf-factory.* appended with px_IMS_HomeDomainName
Referred-by addr-spec	-- check this *sip:master@conference.com*
To addr-spec tag	 SIP URI of the user invited to the conference no tag given
Call-ID callid	 any value according to Call-ID syntax can be used
CSeq value	 any value according to CSeq syntax can be used

202 Accepted for REFER (Step 2)

Use the default message “202 Accepted” in annex A.3.3.

INVITE (Step 3)

Use the default message “INVITE for MO call setup” in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
To	
addr-spec	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
Referred-by	
addr-spec	*sip:master@conference.com*
Supported	
option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=*(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 4] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 2] - *a=pcfg:1 t=1* [Note 2] - *a=rtpmap: (*payload type*) H264/90000* - *a=fmtp:* (format) *profile-level-id=42e00c; sprop-parameter \ sets=J0LgDJWgUH6Af1A=,KM46gA==* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The tcap/pcfg attributes are present if RTP/AVP is present on the m line. Note 3: The AMR channel number shall be "/1" or omitted. Note 4: Values from 0 to 220 are allowed

100 Trying for INVITE (Step 4)

Use the default message “100 Trying for INVITE” in annex A.2.2.

NOTIFY (Step 5)

Use the default message “MO NOTIFY for refer package” in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

183 Session Progress for INVITE (Step 7)

Use the default message "183 Session Progress for INVITE" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Require	
option-tag	*precondition*
Contact	
addr-spec	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
Message-body	The following SDP types and values. Session description: - *v=0* - *o=1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) AMR-*WB*/16000/1 [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* - *a=inactive* [Note 3] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* - *a=inactive* [Note 3] Media description: - *m=video (transport port) RTP/AVPF* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=acfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* [Note 1] - *a=fmtp:* (format) (format specific parameters) [Note 1] - *a=inactive* [Note 3] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, bandwidth, payload type, format and format specific parameters copied from step 3. Note 2: Present if tcap/pcfg attributes were included in step 3. Note 3: The attribute a=inactive shall be present if it was included in step 3.

PRACK (Step 8)

Use the default message “PRACK” in annex A.2.4 with the exception that either Supported or Require header shall contain the "precondition" and:

Header/param	Value/remark
Content-Type media-type	header shall be present only if there is SDP in message-body *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this request and if there is a message-body length of message-body
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id=42e00c; sprop-parameter \ sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one Note 3: The AMR channel number shall be “/1” or omitted.

200 OK for PRACK (Step 9)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	header shall be present only if there is SDP in message-body *application/sdp*
Content-Length value	 length of message-body
Message-body	Header present if Prack (step 8) contained SDP. Contents if present: SDP body of the 200 response copied from the received PRACK and modified as follows: "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: *a=curr:qos remote sendrecv*

UPDATE (Step 10) optional step used when PRACK contained a=curr:qos local none

Use the default message “UPDATE” in annex A.2.5 with the exception that either Supported or Require header shall contain the "precondition" tag.

Header/param	Value/remark
Message-body	Same contents as specified in step 8.

200 OK for UPDATE (Step 11) - optional step used when UE sent UPDATE

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: *- a=curr:qos remote sendrecv*

200 OK for INVITE (Step 12)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName

ACK (Step 13)

Use the default message “ACK” in annex A.2.7.

NOTIFY (Step 13)

Use the default message “MO NOTIFY for refer package” in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

SUBSCRIBE (Step 13)

Use the default message "SUBSCRIBE for conference event package" in annex A.5.1.

200 OK for NOTIFY (Step 14)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

200 OK for SUBSCRIBE (Step 15)

Use the default message "200 OK for SUBSCRIBE" in annex A.5.2.

NOTIFY (Step 16)

Use the default message "NOTIFY for conference event package" in annex A.5.3 with condition A3.

200 OK for NOTIFY (Step 17)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

BYE (Step 18)

Use the default message "BYE" in annex A.2.8.

200 OK for BYE (Step 19)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1

NOTIFY (Step 20)

Use the default message "NOTIFY for conference event package" in annex A.5.3 with condition A4.

200 OK for NOTIFY (Step 21)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

15.21b.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 3: the UE shall send an INVITE message with correct content according to the Specific Message Contents above.

Step 8: the UE shall send a PRACK request with the correct content according to the Specific Message Contents above.

Step 10: the UE may conditionally send an UPDATE request with the correct content according to the Specific Message Contents above.

15.21c Three way session creation / Video

15.21c.1 Definition

Test to verify that the UE support Three Way Session creation for Video. This process is described in Section 5.3.1.3.3 of 3GPP TS 24.147 [84].

15.21c.2 Conformance requirement

[TS 24.147 clause 5.3.1.3.3]:

When a user is participating in two or more SIP sessions and wants to join together two of these active sessions to a so-called three-way session, the user shall perform the following steps.

1) create a conference at the conference focus by sending an INVITE request with the conference factory URI for the three-way session towards the conference focus, as described in subclause 5.3.1.3.2;

2) decide and perform for each of the active sessions that are requested to be joined to the three-way session, how the remote user shall be invited to the three-way session, which can either be:

   a) by performing the procedures for inviting a user to a conference by sending an REFER request to the user, as described in subclause 5.3.1.5.2; or

   b) by performing the procedures for inviting a user to a conference by sending a REFER request to the conference focus, as described in subclause 5.3.1.5.3;

3) release the active session with the user, by applying the procedures for session release in accordance with RFC 3261 [7], provided that a BYE request has not already been received, after a NOTIFY request has been received, indicating that the user has successfully joined the three-way session, i.e. including:

   a) a body of content-type "message/sipfrag" that indicates a "200 OK" response; and,

   b) a Subscription-State header set to the value "terminated"; and,

4) treat the created three-way session as a normal conference, i.e. the conference participant shall apply the applicable procedures of subclause 5.3.1 for it.

Reference(s)

3GPP TS 24.147 [84]

15.21c.3 Test purpose

1) To verify that the invoking UE is able to create a three-way session by sending a REFER request to the conference focus to inviting a user to a conference;

15.21c.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.8.3-1, steps 1 to 15.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO Video call.

Test procedure

1-4) Call hold is initiated on the UE. The same steps defined in Annex C.8 are used to put the call into hold.

5-17) A new session is created by using the steps defined in Annex C.25.

17A) The UE is triggered to start a multiparty call. This causes the UE to first put the second call on hold as described in Steps 17B-17E, and then to initiate the following steps 19-46D.

17B-17E) The UE puts the second call on hold by executing the steps described in Annex C.8

19-30) UE initiates the conference creation process by executing steps 2-13 of the generic test procedure in Annex C.38.

31-38) UE invites one of the user who have session with the UE to the conference by performing the same procedure as in Annex C.37.

39-46D) UE invites another user who has a session with the UE to the conference by performing the same procedure as in Annex C.37.

UE shall send two BYE requests to terminate the two initial calls it put on hold.

SS responds to the BYE requests with a valid 200 OK response each.

47) SS sends a BYE request to the UE in order to release the active session if BYE request has not already been received.

48) UE responds to the BYE request with valid 200 OK response.

49) SS notifies the UE that its subscription to conf event is terminated.

50) UE responds with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-4			Messages in Annex C.8	The same messages as in Annex C.8 Steps 1-4 are used.
5-17			Steps defined in Annex C.25	The same messages as in Annex C.25 are used.
17A				Make UE start a Multiparty Call
17B-17E			Messages in Annex C.8	The same messages as in Annex C.8 Steps 1-4 are used to put the second call on hold
18				Void
19-30			Steps 2-13 defined in Annex C.38	The same messages as in Annex C.38 are used.
31-38			Steps defined in Annex C.37	The same messages as in Annex C.37 steps 1-8 are used.
39-46	→		Steps defined in Annex C.37	The same messages as in Annex C.37 steps 1-8 are used.
46A	→		BYE	UE shall send a BYE to terminate the first call.
46B	←		200 OK	The SS responds the received BYE with 200 OK
46C	→		BYE	UE shall send a BYE to terminate the second call.
46D	←		200 OK	The SS responds the received BYE with 200 OK
47	←		BYE	The SS releases the active session with BYE
48	→		200 OK	The UE sends 200 OK for BYE
49	←		NOTIFY	If the UE had subscribed to the conference event package, the SS notifies the UE that its subscription to conference event package is terminated
50	→		200 OK	The UE sends 200 OK for NOTIFY (if sent by SS)

NOTE 1: Steps 27-30 (i.e., steps 10-13 of C.10) are optional. Therefore, UE can start with steps 31-46 right away after Step 26. If Steps 27-30 are executed, they can happen in parallel to Steps 31-46.

NOTE 2: The two executions of Annex C.19, i.e., steps 31-38 and steps 39-46, can run in parallel.

NOTE 3: Step 46A can happen any time after step 35. The SS sends the corresponding 200 OK message right after having received the BYE message.

NOTE 4: Step 46C can happen any time after step 43. The SS sends the corresponding 200 OK message right after having received the BYE message.

Specific Message Contents

INVITE(Step 6)

Use the default message “INVITE” in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	px_IMS_CalleeUri2 px_IMS_CalleeUri2 is used to invite another user to the session. px_IMS_CalleeUri2 may be either SIP or Tel URI. It may contain a dialstring and phone-context parameter, when calling to dialstring. When calling to dialstring SIP URI must also contain user=phone or user=dialstring parameter. The dialstring, if used, may be global, home local number or geo-local number. For home local numbers the value of phone-context parameter must equal the home domain name i.e. px_IMS_HomeDomainName. For geo-local numbers the home domain name must be prefixed by string “geo-local.” or access technology specific prefix, if the UE supports that option. Note: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is UE implementation specific. For instance the UE might have a UI setting.
To	
addr-spec	px_IMS_CalleeUri2

183 Session in Progress for INVITE (Step 8)

Use the default message “183 Session in Progress for INVITE” in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

180 Ringing for INVITE (Step 13)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

200 OK for INVITE (Step 11)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

BYE (Step 47)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 48)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

NOTIFY (Step 49)

Use the default message “NOTIFY for conference event package” in annex A.5.3 with condition A4.

200 OK for NOTIFY (Step 50)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

15.21c.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

The UE shall send requests and responses as described in clause 15.21c.4.

15.22 Void

15.23 Void

15.24 Void

15.25 MO Explicit Communication Transfer – Consultative Call Transfer

15.25.1 Definition

Test to verify that the transferor UE correctly performs IMS Multimedia Telephony Consultative Explicit Communication Transfer (ECT). This process is described in 3GPP TS 24.629 [104].

15.25.2 Conformance requirement

[TS 24.629 Rel 12, clause 4.5.2.1]:

A UE that initiates a transfer operation shall:

- issue a REFER request in the original communications dialog as specified in RFC 3515, where:
  - a) the request URI shall contain the SIP URI of the transferee as received in the Contact header field.
  - b) the Refer-To header field shall indicate the public address of the transfer Target.
  - c) in case of consultative transfer, the transferor UE has a consultation communication with the transfer Target, a Replaces header field parameter shall be added to the Refer-To URI together with a Require=replaces header field parameter.
  - d) the Referred-By header field can be used to indicate the identity of the transferor. When privacy was required in the original communications dialog and a Referred-By header field is included, the UE shall include a Privacy header field set to "user".

After the REFER request is accepted by the other end with a 2xx response, the transferor UE should get notifications of how the transferee's communication setup towards the transfer Target is progressing.

When a NOTIFY request is received on the REFER dialog that indicates that the transferee and the transfer Target have successfully setup a communication, the transferor UE may terminate the original communication with the transferee UE, by sending a BYE message on the original dialog.

Reference(s)

3GPP TS 24.629 [104], clause 4.5.2.1.

15.25.3 Test purpose

1) To verify that the transferor UE puts the call on hold before the transfer with a correct exchange of SIP/SDP protocol signalling messages; and

2) To verify that the transferor UE has a consultative communication with the transfer target UE; and

3) To verify that the transferor UE issues a correctly composed REFER request to initiate the call transfer; and

4) To verify that the transferor UE correctly processes the NOTIFYs from the transferee UE; and

5) To verify that the transferor UE correctly processes the BYE request releasing the call with the transfer target UE.

15.25.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up an MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-4) UE is in an active call with the SS (simulating the transferee). Consultative Call Transfer is initiated at the UE. UE puts the ongoing call on hold.

5-16) UE sets up an MO call with the transfer target (also simulated by the SS).

17-20) UE puts the call with the transfer target UE on hold.

21) SS waits for UE to send a REFER request to the transferee within the existing dialog between the UE and the transferee.

22) SS responds to the REFER request with a valid 200 OK response.

23) SS sends UE an initial NOTIFY to indicate that the implicit refer subscription is pending.

24) SS waits for UE to respond to NOTIFY with valid 200 OK response.

25-28) Call between UE and the transferee UE is put on hold by SS.

29) SS releases call between UE and the transfer target by sending a BYE request.

30) SS waits for UE to respond to the BYE request with valid 200 OK response.

31) SS sends UE the final NOTIFY to indicate that the call transfer was successfully completed.

32) SS waits for UE to respond to NOTIFY with valid 200 OK response.

33) UE may send a BYE request to release the call with the transferee UE.

34) If UE has sent a BYE request in Step 33, SS responds to this request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
			Make UE attempt Consultative Call Transfer	
1-4			Steps defined in Annex C.8 to hold the call	UE holds the call with the transferee.
5-16			Steps 2-13 defined in Annex C.21	In order to establish a call with the transfer target, the same messages as in Annex C.21 are used.
17-20			Steps defined in Annex C.8 to hold the call	UE holds call with transfer target.
21	→		REFER	The UE sends REFER to SS, simulating the transferee, referring to the transfer target
22	←		200 OK	The SS responds to REFER with 200 OK
23	←		NOTIFY	The SS, simulating the transferee, sends initial NOTIFY for the implicit subscription created by the REFER request
24	→		200 OK	The UE responds to NOTIFY with 200 OK
25-28			Steps defined in Annex C.9 to hold the call	The SS, simulating the transferee, puts the UE on hold, setting the direction attribute to inactive.
29	←		BYE	The SS, simulating the transfer target, releases the call between UE and the transfer target with BYE
30	→		200 OK	The UE responds to BYE with 200 OK
31	←		NOTIFY	The SS, simulating the transferee, sends a NOTIFY to confirm that the call transfer has been completed
32	→		200 OK	The UE responds to NOTIFY with 200 OK
33	→		BYE	Optional: UE may send BYE request to release call with the transferee
34	←		200 OK	If the UE has sent BYE in step 33 then SS sends 200 OK for BYE

Specific Message Contents

INVITE(Step 5 resp Step 2 of C.21)

Use the default message “INVITE” in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Request-Line Request-URI	 px_IMS_CalleeUri2 px_IMS_CalleeUri2 may be either SIP or Tel URI. It may contain a dialstring and phone-context parameter, when calling to dialstring. When calling to dialstring SIP URI must also contain user=phone or user=dialstring parameter. The dialstring, if used, may be global, home local number or geo-local number. For home local numbers the value of phone-context parameter must equal the home domain name i.e. px_IMS_HomeDomainName. For geo-local numbers the home domain name must be prefixed by string “geo-local.” or access technology specific prefix, if the UE supports that option. Note: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is UE implementation specific. For instance the UE might have a UI setting.
To addr-spec	 px_IMS_CalleeUri2

183 Session in Progress for INVITE (Step 7 resp Step 4 of C.21)

Use the default message "183 Session in Progress for INVITE" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

180 Ringing for INVITE (Step 12 resp Step 9 of C.21)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

200 OK for INVITE (Step 15 resp Step 12 of C.21)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_IMS_CalleeContactUri2

Messages in Steps 17-20

Messages in Steps 17-20 are the same as those specified in Annex C.8 with the following exceptions:

INVITE or UPDATE (Step 17) using condition A5 of A.2.1 (respectively corresponding requirements when using UPDATE) and with the following exceptions

Header/param	Value/remark
Request-Line	
Request-URI	px_IMS_CalleeContactUri2

REFER (Step 21)

Use the default message "MO REFER" in annex A.2.10 on the first dialog created in the preamble with the following exceptions:

Header/param	Value/remark
Refer-To	
value	<public address of transfer target?Replaces=(dialog id of the dialog between the UE and the transfer target)&Require=replaces>
Referred-By	
value	same value as addr-spec field in From header in the first INVITE during initial call setup, if header present
Privacy	
value	user (shall be included if privacy was required during original communication dialog and Referred-By header field is included)

NOTIFY (Step 23)

Use the default message "MT NOTIFY for refer package" in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 24)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1

Messages in Steps 25-28

Messages in Steps 25-28 are the same as those specified in Annex C.9 with the following exceptions:

- each media line shall carry direction attribute "a=inactive".

NOTIFY (Step 31)

Use the default message "MT NOTIFY for refer package" in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Subscription-State substate-value expires reason	 *Terminated* omitted from the request *Noresource*
Message-body	*SIP/2.0 200 OK*

200 OK for NOTIFY (Step 32)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1

15.25.5 Test requirements

None additional.

15.26 Void

15.27 Communication Waiting and answering the call

15.27.1 Definition

Test to verify that the MT UE correctly performs MTSI Communication Waiting. This process is described in 3GPP TS 24.615 [95].

15.27.2 Conformance requirement

Generic requirements for Communication Waiting can be found in subclauses 4.5.5.3.2, 4.5.5.3.3, and 4.5.5.3.4 of TS 24.615.

[TS 24.615 subclause 4.5.5.3.2]:

Upon receipt of an INVITE request containing:

- a Content-Type header field set to "application/vnd.3gpp.cw+xml";

- a MIME body according to subclause 4.4.1 with the with the <communication-waiting-indication> element contained in the <ims-cw> root element; and
- if the maximum number of waiting communications is not reached (i.e. UDUB condition has not occurred), the UE shall:
  - provide a CW indication to the user;
  - send a 180 (Ringing) response to the INVITE request according to the provisional response procedures described in 3GPP TS 24.229 [2];
  - optionally, if the INVITE includes an Expires header field, use the value of this header field to provide the time to expiry information of the communication waiting to the user; and
  - optionally start timer T_{UE-CW};

NOTE 1: The timer T_{UE-CW} is used in order to limit the duration of the CW condition at the UE. For terminals that can provide an indication to the user that a CW condition is occurring without disturbing the active communication, this timer is not needed.

NOTE 2: RFC 5621 [9] describes conditions under which a 415 (Unsupported Media Type) response is returned.

The UE may insert an Alert-Info header field set to "<urn:alert:service:call-waiting>" according to RFC 7462 [131] in the 180 (Ringing) response, according to the provisional response procedures described in 3GPP TS 24.229 [2].

[TS 24.615 subclause 4.5.5.3.3]:

Case A

If user B accepts the waiting communication and holds (per procedures in 3GPP TS 24.610 [5]) or releases (per procedures in 3GPP TS 24.229 [2]) the active communication and timer T_{UE-CW} has not expired, user B's UE shall:

- stop timer T_{UE-CW} (if it has been started);
- stop providing the CW indication to User B; and
- apply the procedures for answering the waiting communication to User B as described in 3GPP TS 24.229 [2].

Case B

If T_{UE-CW} was started and expires, user B's UE shall:

- stop providing the CW indication to User B; and
- send a 480 (Temporarily Unavailable) response towards User C, optionally including a Reason header field set to cause 19, in accordance with RFC 6432 [130].

[TS 24.615 subclause 4.5.5.3.4]:

If user B's UE receives a CANCEL request or BYE request from User C during a CW condition, user B's UE shall:

- stop timer T_{UE-CW} (if necessary);
- stop providing the CW indication to User B; and
- apply the terminating UE procedures upon receipt of CANCEL or BYE as described in 3GPP TS 24.229 [2].

If user B's UE receives a CANCEL request or BYE request from User A and during a CW condition, user B's UE shall:

- stop timer T_{UE-CW} (if necessary);
- stop providing the CW indication to User B;
- apply the terminating UE procedures upon receipt of CANCEL request or BYE request as described in 3GPP TS 24.229 [2]; and
- optionally apply the procedure for accepting the waiting communication as described in 3GPP TS 24.229 [2].

Reference(s)

3GPP TS 24.615 [95], clauses 4.5.5.3.2, 4.5.5.3.3, and 4.5.5.3.4

15.27.3 Test purpose

1) To verify that the invoking UE is able to support the terminal based communication waiting service;

2) To verify that the invoking UE sends 180 (Ringing) response with a Alert-Info header field set to "<urn:alert:service:call-waiting>" in a communication waiting process.

15.27.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE discovered P-CSCF, registered to IMS services and set up an MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in Annex C.21, as described in TS 36.508 [94] table 4.5A.6.3-1, up to its last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-8) Execute steps 1-8 of annex C.11

9) SS receives 180 Ringing from the UE with an Alert-Info header field set to "<urn:alert:service:call-waiting>".

10) SS may send PRACK to the UE to acknowledge the 180 Ringing.

11) SS may receive 200 OK for PRACK from the UE.

11a) The user terminates the previous session manually.

12) UE shall send a BYE request after step11a.

13) SS responds to the BYE request with a 200 OK response.

14) SS expects and receives 200 OK for INVITE from the UE.

15) SS sends ACK to the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.11	MTSI MT speech call
9	→		180 Ringing	The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) The SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
11a				The user terminates the previous session manually
12	→		BYE	The UE shall send a BYE to terminate its previous session.
13	←		200 OK	The SS responds to the BYE request with a valid 200 OK response.
13a				The user accepts the incoming call
14	→		200 OK	The UE responds to INVITE with a 200 OK final response after the user answers the call.
15	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.

Specific Message Contents

180 Ringing (step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Alert-Info	<urn:alert:service:call-waiting>

PRACK (step 10)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (step 11)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

BYE (step 12)

Use the default message "BYE" in annex A.2.8.

200 OK (step 13)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

200 OK (step 14)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

ACK (step 15)

Use the default message "ACK" in annex A.2.7.

15.27.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

The UE shall send requests and responses as described in clause 15.27.4.

15.28 Communication Waiting and cancelling the call

15.28.1 Definition

Test to verify that the UE correctly performs IMS Multimedia Telephony Communication Waiting (CW) terminal based procedure. This process is described in 3GPP TS 24.615 [95].

15.28.2 Conformance requirement

[TS 24.615 clause 1]:

The **Communication Waiting (CW)** service enables a user to be informed, that very limited resources are available for an incoming communication. The user then has the choice of accepting, rejecting or ignoring the waiting call (as per basic call procedures).

[TS 24.615 clause 4.2.1]:

When a communication arrives at the destination user, the UE validates the status of the user. If the user is already involved in one or more communications, the terminal notifies the served user of a communication waiting situation.

[TS 24.615 clause 4.5.5.3.2]:

The UE may insert an Alert-Info header field set to "<urn:alert:service:call-waiting>" according to RFC 7462 [131] in the 180 (Ringing) response, according to the provisional response procedures described in 3GPP TS 24.229.

[TS 24.615 clause 4.5.5.3.4]:

If user B's UE receives a CANCEL request or BYE request from User C during a CW condition, user B's UE shall:

- stop timer $T_{UE\text{-}CW}$ (if necessary);
- stop providing the CW indication to User B; and
- apply the terminating UE procedures upon receipt of CANCEL or BYE as described in 3GPP TS 24.229.

Reference(s)

3GPP TS 24.615 [95] clauses 1, 4.2.1, 4.5.5.3.2 and 4.5.5.3.4

15.28.3 Test purpose

1) To verify that the UE sends a correctly composed Alert-Info header field within its 180 Ringing response, if the user is involved with another IMS session when the INVITE request reaches the UE; and
2) To verify that the UE notifies the user with CW indication while the communication waiting state persists; and
3) To verify that the UE will correctly handle the incoming CANCEL request terminating the INVITE transaction.

15.28.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE, discovered P-CSCF, registered to IMS services and set up an MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in Annex C.21, as described in TS 36.508 [94] table 4.5A.6.3-1, up to its last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-8) Execute steps 1-8 of annex C.11

9) SS shall receive 180 Ringing from the UE. UE shall give communication waiting notification to the user.

10) SS may send PRACK to the UE to acknowledge the 180 Ringing.

11) SS may receive 200 OK for PRACK from the UE.

12) After 5 seconds SS sends a CANCEL request to terminate the pending INVITE transaction

13) SS expects and receives 200 OK for CANCEL from the UE.

14) SS expects and receives 487 Request Terminated for INVITE from the UE.

15) SS sends ACK to the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.11	MTSI MT speech call
9	→		180 Ringing	The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
12	←		CANCEL	SS sends CANCEL request to terminate the INVITE transaction
13	→		200 OK	The UE acknowledges the CANCEL with 200 OK.
14	→		487 Request Terminated	The UE responds to INVITE with a 487 Request Terminated final response after transaction was terminated.
15	←		ACK	The SS acknowledges the receipt of 487 Request Terminated for INVITE.

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable.
Steps 13 and 14 can occur in any order.

Specific Message Content

180 Ringing (step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exception:

The response shall contain Alert-Info header field with value "<urn:alert:service:call-waiting>"

PRACK (step 10)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (step 11)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

CANCEL (step 12)

Use the default message "CANCEL" in annex A.2.15.

200 OK (step 13)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

487 Request Terminated (step 14)

Use the default message "487 Request Terminated" in annex A.2.16.

ACK (step 15)

Use the default message "ACK" in annex A.2.7.

15.28.5 Test requirements

The UE shall send requests and responses as described in clause 15.28.4.

UE shall notify the user about communication waiting until the INVITE transaction is terminated by CANCEL.

15.29 GBA authentication

15.29.1 Definition

Test to verify that the UE activates GBA according TS 24.109 [119]. The IMS Multimedia Telephony Originating Identification Presentation is used as trigger.

15.29.2 Conformance requirement

[TS 24.109 clause 4.2]:

The UE shall initiate the bootstrapping procedure when:

a) the UE wants to interact with a NAF and bootstrapping is required;

b) a NAF has requested bootstrapping required indication as described in subclause 5.2.4 or bootstrapping renegotiation indication as described in subclause 5.2.5; or

c) the lifetime of the key has expired in the UE if one or more applications are using that key.

A UE and the BSF shall establish bootstrapped security association between them by running bootstrapping procedure. Bootstrapping security association consists of a bootstrapping transaction identifier (B-TID) and key material Ks. Bootstrapping session on the BSF also includes security related information about subscriber (e.g. user's private identity). Bootstrapping session is valid for a certain time period, and shall be deleted in the BSF when the session becomes invalid.

Bootstrapping procedure shall be based on HTTP Digest AKA as described in 3GPP TS 33.220 [1] and in RFC 3310 [6] with the modifications described below.

The BSF address is derived from the IMPI or IMSI according to 3GPP TS 23.003 [7].

A UE shall indicate to the BSF that it supports the use of TMPI as defined in 3GPP 33.220 [1] by including a "product" token in the "User-Agent" header field (cf. RFC 2616 [14]) that is set to a static string "3gpp-gba-tmpi" in HTTP requests sent to the BSF.

A BSF shall indicate to the UE that it supports the use of TMPI as defined in 3GPP 33.220 [1] by including a "product" token in the "Server" header field (cf. RFC 2616 [14]) that is set to a static string "3gpp-gba-tmpi" in HTTP responses sent to the UE.

In the bootstrapping procedure, Authorization, WWW-Authenticate, and Authentication-Info HTTP headers shall be used as described in RFC 3310 [6] with following exceptions:

a) the "realm" parameter shall contain the network name where the username is authenticated;

b) the quality of protection ("qop") parameter shall be "auth-int"; and

c) the "username" parameter shall contain user's private identity (IMPI).

NOTE: If the UE does not have an ISIM application with an IMPI, the IMPI will be constructed from IMSI, according to 3GPP TS 23.003 [7].

In addition to RFC 3310 [6], the following apply:

a) In the initial request from the UE to the BSF, the UE shall include Authorization header with following parameters:

- the username directive, set to

  1) the value of the TMPI if one has been associated with the private user identity as described in 3GPP 33.220 [1]; or

  2) the value of the private user identity;

- the realm directive, set to the BSF address derived from the IMPI or IMSI according to 3GPP TS 23.003 [7];

- the uri directive, set to either absoluteURL "http://<BSF address>/" or abs_path "/", and which one is used is specified in RFC 2617 [9];

- the nonce directive, set to an empty value; and

- the response directive, set to an empty value;

b) In the challenge response from the BSF to the UE, the BSF shall include parameters to WWW-Authenticate header as specified in RFC 3310 [6] with following clarifications:

- the realm directive, set to the BSF address derived from the IMPI or IMSI according to 3GPP TS 23.003 [7];

c) In the message from the BSF to the UE, the BSF shall include bootstrapping transaction identifier (B-TID) and the key lifetime to an XML document in the HTTP response payload. The BSF may also include additional server specific data to the XML document. The XML schema definition of this XML document is given in Annex C.

d) When responding to a challenge from the BSF, the UE shall include an Authorization header containing a realm directive set to the value as received in the realm directive in the WWW-Authenticate header.

e) Authentication-Info header shall be included into the subsequent HTTP response after the BSF concluded that the UE has been authenticated. Authentication-Info header shall include the "rspauth" parameter.

After successful bootstrapping procedure the UE and the BSF shall contain the key material (Ks) and the B-TID. The key material shall be derived from AKA parameters as specified in 3GPP TS 33.220 [1]. In addition, BSF shall also contain a set of security specific attributes related to the UE.

An example flow of successful bootstrapping procedure can be found in clause A.3.

Reference(s)

3GPP TS 24.109 [119], clause 4.2.

15.29.3 Test purpose

1) To verify that the UE can perform GBA authentication; and

2) To verify that the UE fulfils the GBA protocol details.

15.29.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with shared secret key of IMS AKA algorithm for XCAP, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

Test procedure

The UE uses GBA as XCAP authentication scheme, GBA bootstrapping exchange is performed according to Annex C.29.2.

The generic test procedure according to annex C.29.1 and C.29.2 are applied: At step 1 activation of Originating Identification Presentation, at step 7 deactivation of Originating Identification Presentation is respectively triggered at the UE.

15.29.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme GBA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

15.30 User initiated USSI

15.30.1 Definition

Test to verify that the UE correctly performs user initiated USSI. This process is described in 3GPP TS 24.390 [152], clauses 4.5.

15.30.2 Conformance requirement

[TS 24.390, clause 4.5.1]:

In the IM CN subsystem USSD messages can be transported in SIP INFO requests, SIP INVITE requests and SIP BYE requests, using a application/vnd.3gpp.ussd+xml MIME body.

Figure 4.1, figure 4.2, figure 4.3 and figure 4.4 give an overview of the supported USSD operations:

```
UE                                                                USSI AS
                                  INVITE
   ---------------------------------------------------------------------->
                           language, ussd-String

                                   BYE
   <----------------------------------------------------------------------
                           language, ussd-String

                                   BYE
   <- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
                                  Error
```

Figure 4.1: UE initiated USSD operation, network does not request further information

[TS 24.390, clause 4.5.2]:

When a UE sends an initial INVITE request, in order to establish a USSD session, it shall include an SDP offer with one media description, according to subclause 6.1.2 of 3GPP TS 24.229 [6]. The UE shall add a zero port number value to the media descriptions of the SDP offer, in order to inform network entities that media resources are not requested for the session.

A pre-existing network initiated USSD session cannot be used to carry a user initiated USSD session.

When the USSI AS sends an SDP answer, it shall also add a zero port number value to any media description received in the associated SDP offer.

[TS 24.390, clause 4.5.3]:

If:

1) the domain selection for originating voice calls specified in 3GPP TS 23.221 [y] determines that the UE uses the IMS to originate voice calls; and

2) the UE is not configured with HPLMN operator preference for invocation of originating USSD requests using CS domain (e.g. see 3GPP TS 24.391 [13]);

or if the UE does not support the CS domain, then the UE can invoke the procedures in subclause 4.5.4, otherwise the UE shall not invoke the procedures in subclause 4.5.4.

[TS 24.390, clause 4.5.4.1]:

NOTE 1: The Content-Language SIP header field is not used to determine the language of the USSD string. Only the <language> XML element is used.

In order to send the initial USSD message, the UE shall send an initial INVITE request, according to 3GPP TS 24.229 [6]. The UE shall populate the request as follows:

1) Request-URI set to a SIP URI with user part including the USSD string and a "phone-context" parameter set to the home network domain name used in REGISTER request according to TS 24.229 [6], a host part set to the home netwok domain name used in REGISTER request as defined in TS 24.229 [6] a "user" URI parameter set to value "dialstring" as specified in RFC 4967 [7];

2) Recv-Info header field containing the g.3gpp.ussd info-package name;

3) Accept header field containing the application/vnd.3gpp.ussd+xml, application/sdp and multipart/mixed MIME types;

4) the Content-Type header, which shall contain "multipart/mixed";

5) SDP offer as described in subclause 4.5.2; and

6) application/vnd.3gpp.ussd+xml MIME body as described in subclause 5.1.3 with a Content-Disposition header field set to "render" and with "handling" header field parameter set to "optional". The XML document shall contain a single <ussd-string> element and may contain a <language> element.

…

When receiving a BYE request containing application/vnd.3gpp.ussd+xml MIME body, the UE shall, in addition to the procedures specified in 3GPP TS 24.229 [6], handle the application/vnd.3gpp.ussd+xml MIME body.

NOTE 2: According to 3GPP TS 24.229 [6], the UE can receive a BYE request without the application/vnd.3gpp.ussd+xml MIME body and in this case the dialog is terminated immediately.

When receiving a 404 (Not Found) response to INVITE request, the UE shall determine that an attempt to deliver the USSD request using IMS fails due to missing network support.

NOTE 3: 3GPP TS 23.221 [14] gives requirements related to failure of the USSD request using IMS due to missing network support.

[TS 24.390, clause 4.5.4.2]:

In addition to the procedures specified in this subclause, the USSI AS shall support the procedures specified in 3GPP TS 24.229 [6] for an AS.

NOTE 1: The Content-Language SIP header field is not used to determine the language of the USSD string. Only the <language> XML element is used.

Upon receiving an initial INVITE request with Request-URI containing the SIP URI including the USSD string and a "user" URI parameter set to value "dialstring" as specified in RFC 4967 [7], if the application/vnd.3gpp.ussd+xml MIME body contained in the request is accepted by the USSI AS, the USSI AS shall:

…

2) send 200 (OK) response to the request following the procedures specified for AS acting as a terminating UA in 3GPP TS 24.229 [6]. The USSI AS shall populate the 200 (OK) response to the request as follows:

   a) Recv-Info header field containing the g.3gpp.ussd info-package name;

   b) Accept header field containing the application/vnd.3gpp.ussd+xml, application/sdp and multipart/mixed MIME types; and

   c) SDP answer as described in subclause 4.5.2.

Upon receiving an ACK request associated with the INVITE request, the USSI AS shall:

…

2) if the network successfully performed the USSD information and does not need any further information, send a BYE request in order to terminate the dialog. The USSI AS shall populate the BYE request with application/vnd.3gpp.ussd+xml MIME body, as described in subclause 5.1.3 including a <ussd-string> element and a <language> element; and

3) if the network informs the UE that the network is unable to process the USSD request or the network informs the UE that the network rejects the USSD request, send a BYE request in order to terminate the dialog. The USSI AS shall populate the BYE request with application/vnd.3gpp.ussd+xml MIME body, as described in subclause 5.1.3, including, a <error-code> element.

Reference(s)

3GPP TS 24.390 [152], clauses 4.5.1, 4.5.2, 4.5.3, 4.5.4.1 and 4.5.4.2.

15.30.3 Test purpose

1) To verify that when originating user initiated USSI the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that when originating user initiated USSI the UE performs the correct exchange of SDP messages.

15.30.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an user initiated USSI with USSD string "*#60#"	The SS may use AT command "CUSD" to trigger the user initiated USSI
2	→		INVITE	UE sends INVITE with the SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		200 OK	SS sends a 200 OK.
5	→		ACK	UE acknowledges.
6	←		BYE	SS sends BYE to release the session.
7	→		200 OK	UE sends a 200 OK.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE" in annex A.2.1 with condition A4 and the following exception.

Header/param	Value/remark
Request-Line Request-URI	 Request-URI set to a SIP URI with user part including the percent-encoded USSD string as used at step 1 and a "phone-context" parameter set to the home network domain name used in REGISTER request, a host part set to the home netwok domain name used in REGISTER request and a "user" URI parameter set to value "dialstring"
To addr-spec tag	 same as Request URI not present
Recv-Info Info-package-type	 *g.3gpp.ussd*
Accept	*application/vnd.3gpp.ussd+xml, application/sdp, multipart/mixed*
Content-Type	
media-type	*multipart/mixed;boundary*=any value
Message-body	The following SDP types and values. --boundary value (as provided in SIP hdr Content-Type) Content-Type: application/sdp Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m*=(media) 0 [Note2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) --boundary value (as provided in SIP hdr Content-Type) *Content-Type: application/vnd.3gpp.ussd+xml* *<?xml version="1.0" encoding="UTF-8"?>* *<ussd-data>* *<language>*(language)*</language>* [Note 3] *<ussd-string>*(USSD string as used at step 1)*</ussd-string>* *</ussd-data>* --boundary value (as provided in SIP hdr Content-Type) Note 1: At least one "c=" field shall be present. Note 2: media is the type of media like *audio.* Note 3: language is the type of USSD language coded as defined in IETF RFC 5646 [153]

200 OK for INVITE (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exception.

Header/param	Value/remark
Recv-Info Info-package-type	 *g.3gpp.ussd*
Accept	*application/vnd.3gpp.ussd+xml, application/sdp, multipart/mixed MIME types*
Content-Type media-type	 *application/sdp*
Message-body	SDP body of the 200 response copied from the received INVITE and modified as follows: - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - IP address on "c=" line changed to indicate to which IP address and port the UE should start sending the media; - "a=" lines are all removed.

BYE (Step 6)

Use the default message "BYE" in annex A.2.8 with the following exception.

Header/param	Value/remark
Content-Type	
media-type	*application/vnd.3gpp.ussd+xml*
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<ussd-data>* *<language>en</language>* *<ussd-string>148*7#</ussd-string>* *</ussd-data>*

15.30.5 Test requirements

SS shall check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

16 Codec selecting

16.1 Void

16.2 Speech AMR, indicate selective codec modes

16.2.1 Definition

Test to verify that the UE correctly performs IMS Multimedia Telephony speech call setup when selective AMR codec modes are offered. This process is described in 3GPP TS 24.173 [65], TS 24.229 [10] and TS 26.114 [66].

16.2.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 24.229, clause 6.1.1]

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229 [10] clause 5.1.4.1. TS 26.114 [66] clauses 5.2.1, 6.2.5, and 7.3.1.

16.2.3 Test purpose

1) To verify that, when initiating MT MTSI speech AMR call with selective codec modes and with the remote UE already having resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

16.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

1) SS sends an INVITE request to the UE.

2) Void.

3) SS may receive 100 Trying from the UE.

3A) SS may receive 183 Session Progress from the UE.
SS triggers the activation of a dedicated bearer.

3B) SS may send PRACK to the UE to acknowledge the 183 Session Progress.

3C) SS may receive 200 OK for PRACK from the UE.

4) SS may receive 180 Ringing from the UE.

5) SS may send PRACK to the UE to acknowledge the 180 Ringing.

6) SS may receive 200 OK for PRACK from the UE.

6A) The UE accepts the session invite.
If 180 Ringing is not received from the UE after 5s from step 1, the MMI command shall be started to trigger the UE to accept the call.

7) SS expects and receives 200 OK for INVITE from the UE.

8) SS send an ACK to acknowledge receipt of the 200 OK for INVITE

9) SS sends BYE to the UE.

10) SS expects and receives 200 Ok for BYE from the UE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
3A	→		183 Session Progress	(Optional) The UE sends 183 response reliably with the SDP answer to the offer in INVITE
3B	←		PRACK	(Optional) SS acknowledges if a 183 Session Progress is received.
3C	→		200 OK	(Optional) The UE responds if a PRACK is sent.
4	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
5	←		PRACK	(Optional) SS shall send PRACK if the 180 response contains 100rel option-tag in the Require header.
6	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
6A				Make UE accept the speech AMR offer.
7	→		200 OK	The UE responds INVITE with 200 OK.
8	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
9	←		BYE	The SS releases the call with BYE.
10	→		200 OK	The UE sends 200 OK for BYE.

NOTE 1: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable

NOTE 2: Steps 4, 5, and 6 can happen in parallel to steps 3B and 3C

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-set=0,2,4,7; mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying for INVITE (Step 3)

183 Session Progress (Step 3A)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=(session name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted.

180 Ringing (Step 4)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	optional if 183 Session Progress is not used not present if 183 Session Progress is used (step 3A) Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=(session name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) *mode-set=0,2,4,7;* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be "/1" or omitted.

200 OK for INVITE (Step 7)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	not present if 183 Session Progress is used (step 3A) or 180 Ringing (step 4) contained SDP. present if 183 Session Progress is not used (step 3A) and 180 Ringing (step 4) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 4.

16.2.5 Test requirements

The UE shall send requests and responses as described in clause 16.2.4.

16.3 Speech AMR-WB, indicate all codec modes

16.3.1 Definition

Test to verify that the UE correctly performs IMS Multimedia Telephony speech call setup when all AMR-WB codec modes are offered. This process is described in 3GPP TS 24.173 [65], TS 24.229 [10] and TS 26.114 [66].

16.3.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

…

MTSI terminals offering wideband speech communication at 16 kHz sampling frequency shall support:

- AMR wideband codec (3GPP TS 26.171, 3GPP TS 26.190, 3GPP TS 26.173 and 3GPP TS 26.204) including all 9 modes and source controlled rate operation 3GPP TS 26.193. The terminal shall be capable of operating with any subset of these 9 codec modes.

…

MTSI terminals offering wideband speech communication shall also offer narrowband speech communications. When offering both wideband speech and narrowband speech communication, wideband shall be listed as the first payload type in the m line of the SDP offer (RFC 4566).

[TS 24.229, clause 6.1.1]

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229 [10] clause 5.1.4.1, TS 26.114 [66] clauses 5.2.1, 6.2.5, and 7.3.1.

16.3.3 Test purpose

1) To verify that, when initiating MT MTSI speech AMR-WB call and with the remote UE already having resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

16.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

1) SS sends an INVITE request to the UE.

2) Void.

3) SS may receive 100 Trying from the UE.

4) SS may receive 183 Session Progress from the UE.
SS triggers the activation of a dedicated bearer.

5) SS may send PRACK to the UE to acknowledge the 183 Session Progress.

6) SS may receive 200 OK for PRACK from the UE.

7) Void.

8) Void.

9) SS may receive 180 Ringing from the UE.

10) SS may send PRACK to the UE to acknowledge the 180 Ringing.

11) SS may receive 200 OK for PRACK from the UE.

11A) The UE accepts the session invite.
If 180 Ringing is not received from the UE after 5s from step 1, the MMI command shall be started to trigger the UE to accept the call.

12) SS expects and receives 200 OK for INVITE from the UE.

13) SS send an ACK to acknowledge receipt of the 200 OK for INVITE

14) SS sends BYE to the UE.

15) SS expects and receives 200 Ok for BYE from the UE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
4	→		183 Session Progress	(Optional) The UE sends 183 response reliably with the SDP answer to the offer in INVITE
5	←		PRACK	(Optional) SS acknowledges if a 183 Session Progress is received.
6	→		200 OK	(Optional) The UE responds if a PRACK is sent.
7	←		Void	
8	→		Void	
9	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) SS shall send PRACK if the 180 response contains 100rel option-tag in the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
11A				Make UE accept the speech AMR WB offer.
12	→		200 OK	The UE responds INVITE with 200 OK.
13	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
14	←		BYE	The SS releases the call with BYE.
15	→		200 OK	The UE sends 200 OK for BYE.

NOTE 1: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable.

NOTE 2: Steps 9, 10, and 11 can happen in parallel to steps 5 and 6.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN (addrtype) (connection-address for SS)* - *b=AS:49* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *b=AS:49* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying for INVITE (Step 3)

Use the default message “100 Trying for INVITE” in annex A.2.2

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

<table>
<tr><th>Header/param</th><th>Value/remark</th></tr>
<tr><td>Status-Line
Reason-Phrase</td><td>
Not checked</td></tr>
<tr><td>Require
option-tag</td><td>
precondition</td></tr>
<tr><td>Message-body</td><td>The following SDP types and values shall be present.

Session description:
- v=0
- o=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE)
- s=(session name)
- c=IN (addrtype) (connection-address for UE) [Note 1]
- b=AS: (bandwidth-value)

Time description:
- t=0 0

Media description:
- m=audio (transport port) RTP/AVP (fmt)
- c=IN (addrtype) (connection-address for UE) [Note 1]
- b=AS: (bandwidth-value)
- b=RS: (bandwidth-value)
- b=RR: (bandwidth-value)

Attributes for media:
- a=rtpmap:(payload type) AMR-WB/16000 [Note 2]
- a=fmtp:(format)

Attributes for preconditions:
- a=curr: a=curr:qos local none
- a=curr:qos remote sendrecv
- a=des:qos mandatory local sendrecv
- a=des:qos mandatory remote sendrecv

Note 1: At least one "c=" field shall be present.
Note 2: The AMR channel number shall be “/1” or omitted.</td></tr>
</table>

PRACK (step 5)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message.

200 OK (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

180 Ringing (Step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	optional if 183 Session Progress is not used not present if 183 Session Progress is used (step 4) Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=(session name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be "/1" or omitted.

PRACK (step 10)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

200 OK for INVITE (Step 12)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	not present if 183 Session Progress is used (step 4) or 180 Ringing (step 9) contained SDP. present if 183 Session Progress is not used (step 4) and 180 Ringing (step 9) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 9.

ACK (Step 13)

Use the default message "ACK" in annex A.2.7.

BYE (step 14)

Use the default message "BYE" in annex A.2.8.

200 OK (step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

16.3.5 Test requirements

The UE shall send requests and responses as described in clause 16.3.4.

16.4 Speech AMR-WB, indicate selective codec modes

16.4.1 Definition

Test to verify that the UE correctly performs IMS Multimedia Telephony speech call setup when selective AMR-WB codec modes are offered. This process is described in 3GPP TS 24.173 [65], TS 24.229 [10] and TS 26.114 [66].

16.4.2 Conformance requirement

Same as 34.229-1 clause 16.3.2.

16.4.3 Test purpose

1) To verify that, when initiating MT MTSI speech AMR-WB call with selective codec modes and with the remote UE already having resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

16.4.4 Method of test

Same as 34.229-1 clause 16.3.4 except

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *b=AS:38* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *c= IN* (addrtype) (connection-address for SS) - *b=AS:38* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-set=0,1,2; mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-set=0,2,4,7; mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line	
Reason-Phrase	Not checked
Require	
option-tag	*precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=(session name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:* (format) *mode-set=0,1,2;* Attributes for preconditions: - *a=a=curr:qos local none* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted.

180 Ringing (Step 9)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	optional if 183 Session Progress is not used not present if 183 Session Progress is used (step 4) Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=(session name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c= IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) *mode-set=0,1,2;* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted.

200 OK for INVITE (Step 12)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	not present if 183 Session Progress is used (step 4) or 180 Ringing (step 9) contained SDP. present if 183 Session Progress is not used (step 4) and 180 Ringing (step 9) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 9.

16.4.5 Test requirements

The UE shall send requests and responses as described in clause 16.4.4.

16.5 to 16.9 Void

16.10 Void

16.11 Void

16.12 Void

16.13 Void

17 Media use cases

17.1 MO Speech, add video remove video

17.1.1 Definition

Test to verify that the UE is able to add a bidirectional video component to an ongoing IMS Multimedia telephony voice call. This process is described in 3GPP TS 24.229 [10], TS 24.173 [65] and TS 26.114 [66].

17.1.2 Conformance requirement

[TS 24.173, clause 5.2]:

IMS multimedia telephony communication service can support different types of media, including media types listed in 3GPP TS 22.173. The session control procedures for the different media types shall be in accordance with 3GPP TS 24.229 and 3GPP TS 24.247, with the following addition:

a) Multimedia telephony is an IMS communication service and the P-Preferred-Service and P-Asserted-Service headers shall be treated as described in 3GPP TS 24.229. The coding of the ICSI value in the P-Preferred-Service and P-Asserted-Service headers shall be according to subclause 5.1.

[TS 24.229, clause 5.1.2A.1]:

If this is a request within an existing dialog, and the request includes a Contact header field, then the UE should insert the previously used Contact header field.

...

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

[TS 24.229, clause 5.1.3]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

The precondition mechanism should be supported by the originating UE.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources, an originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and
- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

Upon generating an initial INVITE request using the precondition mechanism, the UE should not indicate the requirement for the precondition mechanism by using the Require header mechanism.

NOTE 2: If an UE chooses to require the precondition mechanism, i.e. if it indicates the "precondition" option tag within the Require header, the interworking with a remote UE, that does not support the precondition mechanism, is not described in this specification.

NOTE 3: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 4: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation after a 200 (OK) response has been received for the initial INVITE request, in case the terminating UE does not support the PRACK request (as described in RFC 3262) and does not support the UPDATE request (as described in RFC 3311).

[TS 24.229 Rel-13, clause 5.1.4A.1]:

If the precondition mechanism was used during the session establishment, as described in subclause 5.1.3.1 or 5.1.4.1, the UE shall indicate support of the precondition mechanism during a session modification. If the precondition mechanism was not used during the session establishment, the UE shall not indicate support of the precondition mechanism during a session modification.

In order to indicate support of the precondition mechanism during a session modification, upon generating a re-INVITE request, an UPDATE request with an SDP body, or a PRACK request with an SDP body, the UE shall:

a) indicate the support for the precondition mechanism using the Supported header field mechanism;

b) not indicate the requirement for the precondition mechanism using the Require header field mechanism; and

c) if a re-INVITE request is being generated, indicate the support for reliable provisional responses using the Supported header field mechanism.

[TS 24.229, clause 6.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

In order to fulfil the QoS requirements of one or more media streams, the UE may re-use previously reserved resources. In this case the local preconditions related to the media stream, for which resources are re-used, shall be indicated as met.

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,
- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566, unless the UE knows that the precondition mechanism is supported by the remote UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 and RFC 4032; and
- the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec for one or more media streams, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

[TS 26.114 Rel-8, clause 5.2.2]:

MTSI terminals offering video communication shall support:

ITU-T Recommendation H.263 Profile 0 Level 45.

In addition they should support:

ITU-T Recommendation H.263 Profile 3 Level 45;

MPEG-4 (Part 2) Visual Simple Profile Level 3with the following constraints:

- Number of Visual Objects supported shall be limited to 1.
- The maximum frame rate shall be 30 frames per second.
- The maximum f_code shall be 2.
- The intra_dc_vlc_threshold shall be 0.
- The maximum horizontal luminance pixel resolution shall be 352 pels/line.

  - The maximum vertical luminance pixel resolution shall be 288 pels/VOP.
  - If AC prediction is used, the following restriction applies: QP value shall not be changed within a VOP (or within a video packet if video packets are used in a VOP). If AC prediction is not used, there are no restrictions to changing QP value.

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC Baseline Profile Level 1.1 with constraint_set1_flag=1 and without requirements on output timing conformance (annex C of H.264). Each sequence parameter set of H.264 (AVC) shall contain the vui_parameters syntax structure including the num_reorder_frames syntax element set equal to 0.

[TS 26.114 Rel-10, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile (CBP) Level 1.2.

In addition they should support:

  - ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile Level 3.1.

In addition they may support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

[TS 26.114 Rel-8, clause 6.2.1]:

The session setup for RTP transported media shall determine for each media: IP address(es), RTP profile, UDP port number(s); codec(s); RTP Payload Type number(s), RTP Payload Format(s) and any additional session parameters.

[TS 26.114 Rel-8, clause 6.2.1a.1]

MTSI clients should support SDPCapNeg to be able to negotiate RTP profiles for all media types where AVPF is supported. MTSI clients supporting SDPCapNeg shall support the complete SDPCapNeg framework.

SDPCapNeg is described in [69]. This clause only describes the SDPCapNeg attributes that are directly applicable for the RTP profile negotiation, i.e. the tcap, pcfg and acfg attributes. TS 24.229 [7] may outline further requirements needed for supporting SDPCapNeg in SDP messages.

NOTE: This clause describes only how to use the SDPCapNeg framework for RTP profile negotiation using the tcap, pcfg and acfg attributes. Implementers may therefore (incorrectly) assume that it is sufficient to implement only those specific parts of the framework that are needed for RTP profile negotiation. Doing so would however not be future proof since future versions may use other parts of the framework and there are currently no mechanisms for declaring that only a subset of the framework is supported. Hence, MTSI clients are required to support the complete framework.

[TS 26.114 Rel-8, clause 6.2.1a.2]

For voice and real-time text, SDPCapNeg shall be used when offering AVPF the first time for a new media type in the session since the support for AVPF in the answering client is not known at this stage. For video, an MTSI client shall either offer AVPF and AVP together using SDPCapNeg, or the MTSI client shall offer only AVPF, without using SDPCapNeg. If an MTSI client has offered only AVPF for video, and then receives as response either an SDP answer where the video media component has been rejected, or an SIP 488 or 606 failure response with an SDP body indicating that only AVP is supported for video media, the MTSI client should send a new SDP offer with AVP as transport for video. Subsequent SDP offers, in a re-INVITE or UPDATE, may offer AVPF without SDPCapNeg if it is known from an earlier re-INVITE or UPDATE that the answering client supports this RTP profile. If the offer includes only AVP then SDPCapNeg does not need to be used, which can occur for: text; speech if RTCP is not used; and in re-INVITEs or UPDATEs where the RTP profile has already been negotiated for the session in a preceding INVITE or UPDATE.

When offering AVP and AVPF using SDPCapNeg, the MTSI client shall offer AVP on the media (m=) line and shall offer AVPF using SDPCapNeg mechanisms. The SDPCapNeg mechanisms are used as follows:

- The support for AVPF is indicated in an attribute (a=) line using the transport capability attribute ‘tcap’. AVPF shall be preferred over AVP.
- At least one configuration using AVPF shall be listed using the attribute for potential configurations ‘pcfg’.

[TS 26.114, clause 6.2.3]:

If video is used in a session, the session setup shall determine the bandwidth, RTP profile, video codec, profile and level. The "imageattr" attribute as specified in should be supported.

An MTSI terminal shall offer AVPF for all media streams containing video. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 6.2.5]:

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 6.3]:

During session renegotiation for adding or removing media components, the SDP offeror should continue to use the same media (m=) line(s) from the previously negotiated SDP for the media components that are not being added or removed.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556. Therefore, an MTSIclient shall include the "b=RS:" and "b=RR:" fields in SDP, and shall be able to interpret them.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1, 5.1.3, 5.1.4A.1 and 6.1, TS 24.173 [65] clause 5.2 and TS 26.114 [66], clauses 5.2.2, 6.2.1, 6.2.1a.1, 6.2.1a.2, 6.2.3, 6.2.5, 6.3 and 7.3.1.

17.1.3 Test purpose

1) To verify that when adding a video component to an ongoing IMS Multimedia Telephony voice call the UE performs correct exchange of SIP protocol signalling messages; and

2) To verify that within SIP signalling the UE performs correct SDP offer/answer exchanges for negotiating media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1); and

3) To verify that when removing the video component from the IMS Multimedia Telephony call the UE performs correct exchange of SIP and SDP protocol messages.

17.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing annex C.21.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Test procedure

1) Adding video to the voice call is initiated on the UE.

2-10) UE executes the procedure described in TS 36.508 [94] table 4.5A.11.3-1, steps 2 to 7. In detail the following steps are done in IMS.

   2) UE to sends a re-INVITE request to the SS.

   3) SS responds to the re-INVITE request with a 100 Trying response.

4) SS responds to the re-INVITE request with a 183 Session Progress response.

5) SS waits for the UE to send a PRACK request possibly containing the second SDP offer for update of precondition state.

6) SS responds to the PRACK request with a valid 200 OK response.

7) SS waits for the UE to optionally send an UPDATE request containing the final SDP offer. UE will not send the UPDATE request if the PRACK in step 4 already contained the final offer with preconditions met.

8) SS responds to the UPDATE request (if UE sent one) with a valid 200 OK response.

9) SS responds to the re-INVITE request with a valid 200 OK response.

10) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

10A) The UE is triggered to remove the video stream from the multimedia call

11) SS waits the UE to send a re-INVITE request with a SDP offer indicating the removal of the video stream.

12) SS responds to the re-INVITE request with a 100 Trying response.

12A) SS deactivates the EPS bearer corresponding to the video stream and releases the associated radio resources by applying the procedure described in TS 36.508 [94] clause 4.5A.15

13) SS responds to the re-INVITE request with a valid 200 OK response.

14) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for re-INVITE.

15-19) MO Call release according to procedure C.32.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Make UE add video to the voice call.	
2	→		INVITE	UE sends re-INVITE with an SDP offer containing media lines for both voice and video
3	←		100 Trying	The SS responds with a 100 Trying provisional response
4	←		183 Session in Progress	SS responds with an SDP answer indicating that SS has not reserved its resources for video.
5	→		PRACK	UE acknowledges the receipt of 183 response with PRACK and optionally offers second SDP to indicate the changed precondition status.
6	←		200 OK	The SS responds PRACK with 200 OK and answers the second SDP (if any) with mirroring its contents.
7	→		UPDATE	UE sends an UPDATE after having reserved the resources for video if meeting the preconditions was not already indicated in step 2 or 5.
8	←		200 OK	The SS responds UPDATE, if received, with 200 OK and indicates having reserved the resources
9	←		200 OK	The SS responds re-INVITE with 200 OK
10	→		ACK	The UE acknowledges the receipt of 200 OK for re-INVITE
10A			Make UE release video from the media call	
11	→		INVITE	UE sends re-INVITE with a SDP offer indicating that the video component is removed from the call
12	←		100 Trying	The SS responds with a 100 Trying provisional response
12A			SS deactivates the EPS bearer for video	
13	←		200 OK	The SS responds re-INVITE with 200 OK
14	→		ACK	The UE acknowledges the receipt of 200 OK for re-INVITE
15-19			Steps defined in annex C.32	MO Call release

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 4] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 2] - *a=pcfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id=* (att-field) Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The tcap/pcfg attributes are present if RTP/AVP is present on the m line. Note 3: The AMR channel number shall be "/1" or omitted. Note 4: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB*/16000/1 [Note 1] - *a=fmtp:* (format) mode-change-capability=2; max-red=220 [Note 1] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=acfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* [Note 1] - *a=fmtp:* (format) (format specific parameters) [Note 1] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, bandwidth, payload type, format and format specific parameters copied from step 2. Note 2: Present if tcap/pcfg attributes were included in step 2.

PRACK (Step 5)

Use the default message “PRACK” in annex A.2.4 with the exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition* [Note 4]
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id=* (att-field) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one. Note 3: The AMR channel number shall be “/1” or omitted. Note 4: Shall be present if message-body present.

200 OK for PRACK (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 response copied from the received PRACK and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions (video): - *a=curr:qos remote sendrecv*

UPDATE (Step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Supported	Same contents as specified in step 5.
Message-body	Same contents as specified in step 5.

200 OK for UPDATE (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions (video): *- a=curr:qos remote sendrecv*

INVITE (Step 11)

Use the default message "INVITE for MO Call" in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:*(bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Media description: - *m=video 0 RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one. Note 3: The AMR channel number shall be "/1" or omitted.

200 OK (Step 13)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length Value	 length of message-body
Message-body	SDP body of the 200 response copied from the received INVITE and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and, for audio, transport port on "m=" line changed to indicate to which IP address and port the UE should start sending the media;

17.1.5 Test requirements

The UE shall send requests and responses as described in clause 17.1.4

17.2 MT Speech, add video remove video

17.2.1 Definition

Test to verify that the UE correctly adds and removes media video to a mobile terminated speech session video when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clause 5.1.2A.2, TS 24.173 [65] and TS 26.114 [66].

17.2.2 Conformance requirement

[TS 24.229, clause 5.1.2A.2]

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

[TS 24.229 Rel-13, clause 5.1.4A.2]

Upon receiving a re-INVITE request, an UPDATE request, or a PRACK request that indicates support for the precondition mechanism, using the Supported header field or the Require header field, the UE shall:

a) if the precondition mechanism was used during the session establishment, as described in subclause 5.1.3.1 or 5.1.4.1, use the precondition mechanism;

…

If the precondition mechanism is used for the session modification, the UE shall indicate support for the preconditions mechanism, using the Require header field mechanism, in responses that include an SDP body, to the session modification request.

[TS 24.229 release 9 start, clause 6.1.1]

During the session establishment procedure, and during session modification procedures, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

[TS 24.229 release 9 end]

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 26.11 Rel-84, clause 5.2.2]

MTSI terminals offering video communication shall support:

ITU-T Recommendation H.263 Profile 0 Level 45.

In addition they should support:

ITU-T Recommendation H.263 Profile 3 Level 45;

MPEG-4 (Part 2) Visual Simple Profile Level 3with the following constraints:

  - Number of Visual Objects supported shall be limited to 1.
  - The maximum frame rate shall be 30 frames per second.
  - The maximum f_code shall be 2.
  - The intra_dc_vlc_threshold shall be 0.
  - The maximum horizontal luminance pixel resolution shall be 352 pels/line.
  - The maximum vertical luminance pixel resolution shall be 288 pels/VOP.
  - If AC prediction is used, the following restriction applies: QP value shall not be changed within a VOP (or within a video packet if video packets are used in a VOP). If AC prediction is not used, there are no restrictions to changing QP value.

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC Baseline Profile Level 1.1 with constraint_set1_flag=1 and without requirements on output timing conformance (annex C of H.264). Each sequence parameter set of H.264 (AVC) shall contain the vui_parameters syntax structure including the num_reorder_frames syntax element set equal to 0.

[TS 26.114 Rel-10, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile (CBP) Level 1.2.

In addition they should support:

  - ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile Level 3.1.

In addition they may support:

  - ITU-T Recommendation H.263 [22] Profile 0 Level 45.

[TS 26.114, clause 6.2.1a.1]

MTSI clients should support SDPCapNeg to be able to negotiate RTP profiles for all media types where AVPF is supported. MTSI clients supporting SDPCapNeg shall support the complete SDPCapNeg framework.

SDPCapNeg is described in [69]. This clause only describes the SDPCapNeg attributes that are directly applicable for the RTP profile negotiation, i.e. the tcap, pcfg and acfg attributes. TS 24.229 [7] may outline further requirements needed for supporting SDPCapNeg in SDP messages.

NOTE: This clause describes only how to use the SDPCapNeg framework for RTP profile negotiation using the tcap, pcfg and acfg attributes. Implementers may therefore (incorrectly) assume that it is sufficient to implement only those specific parts of the framework that are needed for RTP profile negotiation. Doing so would however not be future proof since future versions may use other parts of the framework and there are currently no mechanisms for declaring that only a subset of the framework is supported. Hence, MTSI clients are required to support the complete framework.

[TS 26.114, clause 6.2.1a.2]

For voice and real-time text, SDPCapNeg shall be used when offering AVPF the first time for a new media type in the session since the support for AVPF in the answering client is not known at this stage. For video, an MTSI client shall either offer AVPF and AVP together using SDPCapNeg, or the MTSI client shall offer only AVPF, without using SDPCapNeg. If an MTSI client has offered only AVPF for video, and then receives as response either an SDP answer where the video media component has been rejected, or an SIP 488 or 606 failure response with an SDP body indicating that only AVP is supported for video media, the MTSI client should send a new SDP offer with AVP as transport for video. Subsequent SDP offers, in a re-INVITE or UPDATE, may offer AVPF without SDPCapNeg if it is known from an earlier re-INVITE or UPDATE that the answering client supports this RTP profile. If the offer includes only AVP then SDPCapNeg does not need to be used, which can occur for: text; speech if RTCP is not used; and in re-INVITEs or UPDATEs where the RTP profile has already been negotiated for the session in a preceding INVITE or UPDATE.

When offering AVP and AVPF using SDPCapNeg, the MTSI client shall offer AVP on the media (m=) line and shall offer AVPF using SDPCapNeg mechanisms. The SDPCapNeg mechanisms are used as follows:

- The support for AVPF is indicated in an attribute (a=) line using the transport capability attribute ‘tcap’. AVPF shall be preferred over AVP.
- At least one configuration using AVPF shall be listed using the attribute for potential configurations ‘pcfg’.

[TS 26.114, clause 6.2.3]

If video is used in a session, the session setup shall determine the bandwidth, RTP profile, video codec, profile and level. The "imageattr" attribute as specified in [76] should be supported.

An MTSI client shall offer AVPF for all media streams containing video. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 6.3]

During session renegotiation for adding or removing media components, the SDP offeror should continue to use the same media (m=) line(s) from the previously negotiated SDP for the media components that are not being added or removed.

[TS 26.114, clause 7.3.1]

…

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

…

Reference(s)

3GPP TS 24.229 [10] clauses 5.1.2A.2, 5.1.4A.2 and 6.1.1 (release 9), TS 26.114 [66] clauses 5.2.1, 5.2.2, 6.2.1a.1, 6.2.1a.2, 6.2.3, 6.2.5, 6.3 and 7.3.1.

NOTE 1: Reference to a specific release is used when a corrected requirement is not updated in earlier releases of the core specifications but applies to these earlier releases.

17.2.3 Test purpose

1) To verify that media video can be added and removed when an MT MTSI speech call is established.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

17.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and established an MT MTSI speech call, by executing the generic test procedure in Annex C.11 steps 1 to 13.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-9) UE executes the procedures described in TS 36.508 [94] table 4.5A.12.3-1, steps 1 to 12. In detail the following steps are done in IMS:

1) SS sends a re-INVITE request to the UE.

2) Void

2a) SS may receive 100 Trying from the UE.

3) SS receives 183 Session Progress from the UE.

4) SS sends PRACK to the UE to acknowledge the 183 Session Progress.

5) SS receives 200 OK for PRACK from the UE.

6) SS sends UPDATE to the UE, with SDP indicating that precondition is met on the server side.

7) SS receives 200 OK for UPDATE from the UE.

7A) The UE accepts the session invite.

8) SS expects and receives 200 OK for re-INVITE from the UE.

9) SS sends ACK to the UE.

10) SS sends a re-INVITE to the UE with a SDP offer indicating that the video component is removed from the call.

11) SS expects and receives 200 OK for re-INVITE from the UE.

11A) SS deactivates the EPS bearer corresponding to the video stream and releases the associated radio resources by applying the procedure described in TS 36.508 [94] clause 4.5A.15

12) SS sends ACK to the UE.

13-16) MT Call release according to procedure C.33

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends re-INVITE with second SDP offer to add video.
2				Void.
2a	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
3	→		183 Session Progress	The UE responds to re-INVITE by sending 183 response reliably with the SDP answer
4	←		PRACK	SS acknowledges the receipt of 183 response from the UE
5	→		200 OK	The UE acknowledges the PRACK with 200 OK.
6	←		UPDATE	SS sends an UPDATE with SDP offer indicating SS reserved resources.
7	→		200 OK	The UE acknowledges the UPDATE with 200 OK and includes SDP answer to acknowledge its current precondition status.
7A				Make UE accept the speech and video offer.
8	→		200 OK	The UE responds to the re-INVITE with a 200 OK final response.
9	←		ACK	The SS acknowledges the receipt of 200 OK for the re-INVITE.
10	←		INVITE	SS sends a re-INVITE with a SDP offer indicating that the video component is removed from the call
10A	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
11	→		200 OK	The UE responds to the re-INVITE with a 200 OK final response.
11A			SS deactivates the EPS bearer for video	
12	←		ACK	The SS acknowledges the receipt of 200 OK for the re-INVITE.
13				Void
14-16			Steps defined in annex C.33	MT Call release

NOTE: The default messages contents in annex A are used with condition “IMS security“or “GIBA” when applicable

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/remark
Supported	
option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:352* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS: 37* - *b=RS: 0* - *b=RR: 2000* Attributes for media: - *a=rtpmap: 97 AMR-WB/16000/1* - *a=fmtp: 97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF 101* - *b=AS: 315* - *b=RS: 0* - *b=RR: 2500* Attributes for media: - *a=rtpmap: 101 H264/90000* - *a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=rtcp-fb:* trr-int 5000* - *a=rtcp-fb:* nack* - *a=rtcp-fb:* nack pli* - *a=rtcp-fb:* ccm fir* - *a=rtcp-fb:* ccm tmmbr* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (step 3)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 3] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *packetization-mode=0;profile-level-id=* (att-field)*); * Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be "/1" or omitted. Note 3: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

PRACK (step 4)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message.

200 OK (step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

UPDATE (step 6)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Supported	
option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:352* Time description: *-t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS: 37* - *b=RS: 0* - *b=RR: 2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF 101* - *b=AS: 315* - *b=RS: 0* - *b=RR: 2500* Attributes for media: - *a=rtpmap: 101 H264/90000* - *a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=rtcp-fb:* trr-int 5000* - *a=rtcp-fb:* nack* - *a=rtcp-fb:* nack pli* - *a=rtcp-fb:* ccm fir* - *a=rtcp-fb:* ccm tmmbr* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 3] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *packetization-mode=0;profile-level-id= (att-field); * Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted. Note 3: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one

200 OK (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

ACK (step 9)

Use the default message "ACK" in annex A.2.7.

INVITE (step 10)

Use the default message “INVITE for MT Call” in annex A.2.9 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: *v=0* "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one *s=-* *c=IN* (addrtype) (connection-address for SS) *b=AS:37* Time description: *t=0 0* Media description: *m=audio* (transport port) *RTP/AVP 97* *b=AS: 37* *b=RS: 0* *b=RR: 2000* Attributes for media: *a=rtpmap:97 AMR-WB/16000/1* *a=fmtp:97 mode-change-capability=2; max-red=220* *a=ptime:20* *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video 0 RTP/AVPF 101* - *b=AS: 315* - *b=RS: 0* - *b=RR: 2500* Attributes for media: - *a=rtpmap: 101 H264/90000* - *a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying (step 10A)

Use the default message "100 Trying for INVITE" in annex A.2.2.

200 OK (step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	SDP body not checked.

ACK (step 12)

Use the default message "ACK" in annex A.2.7.

BYE (step 14)

Use the default message "BYE" in annex A.2.8.

200 OK (step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

17.2.5 Test requirements

The UE shall send requests and responses as described in clause 17.2.4

17.3 to 17.18 Void

18 SMS over IMS

18.1 Mobile Originating SMS

18.1.1 Definition

Test to verify that the UE is able to send a Mobile Originating SMS over IMS and to receive a status report.

18.1.2 Conformance requirement

[TS 24.341, clause 5.3.1.2]:

When an SM-over-IP sender wants to submit an SM over IP, the SM-over-IP sender shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the PSI of the SC of the SM-over-IP sender;

NOTE 1: The PSI of the SC can be SIP URI or tel URI based on operator policy. The PSI of the SC can be obtained using one of the following methods in the priority order listed below:

1) provided by the user;

2) if UICC is used, then:

- if present in the ISIM, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM of the ISIM as per 3GPP TS 31.103 [18];

- if not present on the ISIM, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM of the USIM as per 3GPP TS 31.102 [19]; or

- if neither present on the ISIM nor on the USIM, then the PSI of the SC contains the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM as per 3GPP TS 31.102 [19]. If the PSI of the SC is based on the E.164 number from the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM then the URI constructed can be either a tel URI or a SIP URI (using the "user=phone" SIP URI parameter format).

3) if SIM is used instead of UICC, then the PSI of the SC contains the TS-Service Centre Address stored in the EF_{SMSP} in DF_TELECOM as per 3GPP TS 51.011 [20]. If the PSI of the SC is based on the E.164 number from the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM then the URI constructed can be either a tel URI or a SIP URI (using the "user=phone" SIP URI parameter format); or

4) if neither the UICC nor SIM is used, then how the PSI of the SC is configured and obtained is through means outside the scope of this specification.

b) the From header, which shall contain a public user identity of the SM-over-IP sender;

NOTE 2: The IP-SM-GW will have to use an address of the SM-over-IP sender that the SC can process (i.e. an E.164 number). This address will come from a tel URI in a P-Asserted-Identity header (as defined in RFC 3325 [13]) placed in the SIP MESSAGE request by the P-CSCF or S-CSCF.

NOTE 3: The SM-over-IP sender has to store the Call-ID of the SIP MESSAGE request, so it can associate the appropriate SIP MESSAGE request including a submit report with it.

c) the To header, which shall contain the SC of the SM-over-IP sender;

d) the Content-Type header, which shall contain "application/vnd.3gpp.sms"; and

e) the body of the request shall contain an RP-DATA message as defined in 3GPP TS 24.011 [8], including the SMS headers and the SMS user information encoded as specified in 3GPP TS 23.040 [3].

NOTE 4: The address of the SC is included in the RP-DATA message content. The address of the SC included in the RP-DATA message content is stored in the EF_{SMSP} in DF_TELECOM of the (U)SIM of the SM-over-IP sender.

NOTE 5: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

NOTE 6: Both the address of the SC and the PSI of the SC can be configured in the $EF_{PSISMSC}$ in DF_TELECOM of the USIM and ISIM respectively using the USAT as per 3GPP TS 31.111 [21].

The SM-over-IP sender may request the SC to return the status of the submitted message. The support of status report capabilities is optional for the SC.

When a SIP MESSAGE request including a submit report in the "vnd.3gpp.sms" payload is received, the SM-over-IP sender shall:

- if SM-over-IP sender supports In-Reply-To header usage and the In-Reply-To header indicates that the request corresponds to a short message submitted by the SM-over-IP sender, generate a 200 (OK) SIP response according to RFC 3428 [14].

if SM-over-IP sender supports In-Reply-To header usage and the In-Reply-To header indicates that the request does not correspond to a short message submitted by the SM-over-IP sender, a 488 (Not Acceptable here) SIP response according to RFC 3428 [14].

- if SM-over-IP sender does not support In-Reply-To header usage, generate a 200 (OK) SIP response according to RFC 3428 [14]; and extract the payload encoded according to 3GPP TS 24.011 [8] for RP-ACK or RP-ERROR.

[TS 24,341 clause 5.3.1.3]:

When a SIP MESSAGE request including a status report in the "vnd.3gpp.sms" payload is delivered, the SM-over-IP sender shall:

- generate a SIP response according to RFC 3428 [14];
- extract the payload encoded according to 3GPP TS 24.011 [8] for RP-DATA; and
- create a delivery report for the status report as described in subclause 5.3.2.4. The content of the delivery report is defined in 3GPP TS 24.011 [8].

[TS 24,341 clause 5.3.2.4]:

When an SM-over-IP receiver wants to send an SM delivery report over IP, the SM-over-IP receiver shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the IP-SM-GW;

NOTE 1: The address of the IP-SM-GW is received in the P-Asserted-Identity header in the SIP MESSAGE request including the delivered short message.

b) the From header, which shall contain a public user identity of the SM-over-IP receiver.

c) the To header, which shall contain the IP-SM-GW;

b) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

c) the body of the request shall contain the RP-ACK or RP-ERROR message for the SM delivery report, as defined in 3GPP TS 24.011 [8].

NOTE 2: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

Reference(s)

3GPP TS 24.341[90], clauses 5.3.1.2, 5.3.1.3 and 5.3.2.4.

18.1.3 Test purpose

1) To verify that when sending of a Mobile Originating SMS over IMS is initiated, the UE sends a SIP MESSAGE request constructed as described in 3GPP TS 24.341 [90], clause 5.3.1.2; and

2) To verify that the UE correctly handles reception of a SIP MESSAGE request including a submit report as described in 3GPP TS 24.341 [90], clause 5.3.1.2; and

3) To verify that when receiving a SIP MESSAGE request including a status report, the UE generates the correct SIP response, extracts the payload for RP-DATA and creates a delivery report as described in 3GPP TS 24.341 [90], clause 5.3.1.3.

18.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, and registered to IMS services.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

1) Sending of a Mobile Originating SMS over IMS is initiated at the UE. The SS waits for the UE to send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the short message.

2) The SS responds to the SIP MESSAGE request with a 202 Accepted response.

3) The SS sends a SIP MESSAGE request to the UE including a vnd.3gpp.sms payload that contains a short message submission report indicating a positive acknowledgement of the short message sent by the UE at Step 1).

4) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

5) The SS sends a SIP MESSAGE request to the UE including a vnd.3gpp.sms payload that contains a status report.

6) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

7) The SS waits for the UE to send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a delivery report for the status report received at Step 5).

8) The SS responds to the SIP MESSAGE request with a 202 Accepted response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a short message
2	←		202 Accepted	SS responds with 202 Accepted
3	←		SIP MESSAGE request	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the short message submission report indicating a positive acknowledgement of the short message sent by the UE at Step 1
4	→		200 OK	UE responds with 200 OK
5	←		SIP MESSAGE request	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a status report
6	→		200 OK	UE responds with 200 OK
7	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a delivery report for the status report received at Step 5
8	←		202 Accepted	SS responds with 202 Accepted

NOTE: The default messages contents in annex A are used with condition “IMS security” or “GIBA” when applicable

Specific Message Contents

SIP MESSAGE request (Step 1)

Use the default message “Message for MO SMS” in Annex A.7.3

202 Accepted for SIP MESSAGE request (Step 2)

Use the default message “202 Accepted” in annex A.3.3.

SIP MESSAGE request (Step 3)

Use the default message “Short message submission report for MO SMS” in Annex A.7.4

200 OK for SIP MESSAGE request (Step 4)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

SIP MESSAGE request (Step 5)

Use the default message “Status Report for MO SMS” in Annex A.7.5

200 OK for SIP MESSAGE request (Step 6)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

SIP MESSAGE request (Step 7)

Use the default message “Delivery Report for status report for MO SMS” in Annex A.7.6.

202 Accepted for SIP MESSAGE request (Step 8)

Use the default message “202 Accepted” in annex A.3.3.

18.1.5 Test requirements

SS shall check that the if the UE uses full IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

1) In step 1, the UE shall send a SIP MESSAGE request with the following information:
   a) the Request-URI, which shall contain the Public Service Identity of the SM-SC (value not checked);
   b) the From header, which shall contain a public user identity of the UE;
   c) the To header, which shall contain the same URI as the Request-URI;
   d) the Content-Type header, which shall contain "application/vnd.3gpp.sms"; and
   e) the body of the request shall contain an RP-DATA message as defined in 3GPP TS 24.011, including the SMS headers and the SMS user information encoded as specified in 3GPP TS 23.040.
   f) Mandatory headers Via, Cseq, and max- shall be present
2) In step 4, the UE shall send a 200 OK response.
3) In Step 6, the UE shall send a 200 OK response.
4) In Step 7, the UE shall send a SIP MESSAGE request with the following information:
   a) same Request-URI as used in the P-Asserted-Identity header of the SIP message sent to the UE at step 5;

b) the From header, which shall contain a public user identity of the UE;

c) the To header, which shall contain the IP-SM-GW;

d) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

e) the body of the request shall contain the RP-ACK or RP-ERROR message for the SM delivery report, as defined in 3GPP TS 24.011 [92].

f) Mandatory headers Via, Cseq, and max- shall be present.

18.1a Mobile Originating Concatenated SMS

18.1a.1 Definition

Test to verify that the UE is able to send a Mobile Originating Concatenated SMS over IMS. This process is described in 3GPP TS 23.040 [93], clauses 9.2.3.23, 9.2.3.24 and 9.2.3.24.1 and TS 24.341 [90], clauses 5.3.1.2 .

18.1a.2 Conformance requirement

[TS 23.040, clause 9.2.3.23]:

The TP-User-Data-Header-Indicator is a 1 bit field within bit 6 of the first octet of the following six PDUs:

- SMS-SUBMIT,
- SMS-SUBMIT-REPORT,
- SMS-DELIVER,
- SMS-DELIVER-REPORT,
- SMS-STATUS-REPORT,
- SMS-COMMAND.

TP-UDHI has the following values.

Bit no. 6 0 The TP-UD field contains only the short message

1 The beginning of the TP-UD field contains a Header in addition to the short message.

[TS 23.040, clause 9.2.3.24]:

The length of the TP-User-Data field is defined in the PDU's of the SM-TL (see clause 9.2.2).

The TP-User-Data field may comprise just the short message itself or a Header in addition to the short message depending upon the setting of TP-UDHI.

Where the TP-UDHI value is set to 0 the TP-User-Data field comprises the short message only, where the user data can be 7 bit (default alphabet) data, 8 bit data, or 16 bit (UCS2 [24]) data.

Where the TP-UDHI value is set to 1 the first octets of the TP-User-Data field contains a Header in the following order starting at the first octet of the TP-User-Data field.

Irrespective of whether any part of the User Data Header is ignored or discarded, the MS shall always store the entire TPDU exactly as received.

FIELD	LENGTH
Length of User Data Header	1 octet
Information-Element-Identifier "A"	1 octet
Length of Information-Element "A"	1 octet

Information-Element "A" Data	0 to "n" octets
Information-Element-Identifier "B"	1 octet
Length of Information-Element "B"	1 octet
Information-Element "B" Data	0 to "n" octets
Information-Element-Identifier "X"	1 octet
Length of Information-Element "X"	1 octet
Information-Element "X" Data	0 to "n" octets

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for uncompressed GSM 7 bit default alphabet data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

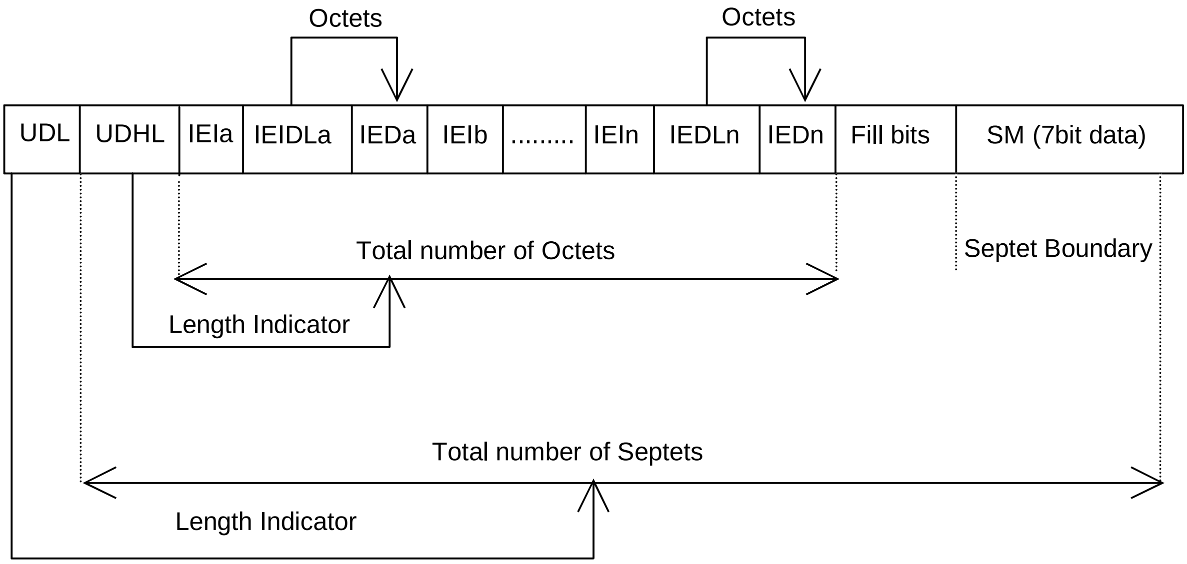

Figure 9.2.3.24 (a)

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for uncompressed 8 bit data or uncompressed UCS2 data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

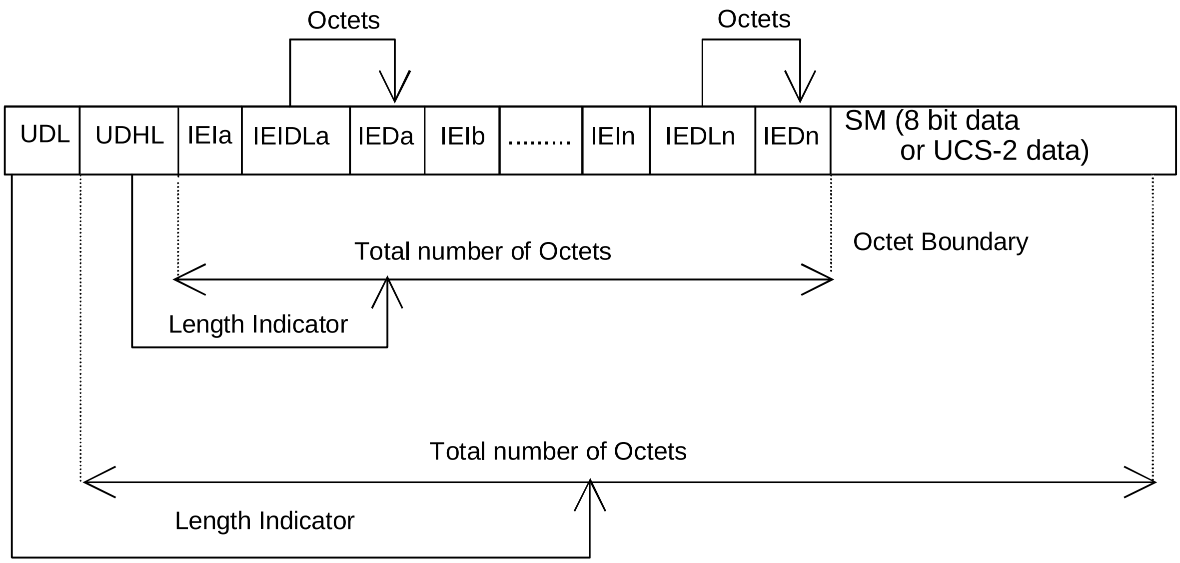

Figure 9.2.3.24 (b)

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for compressed GSM 7 bit default alphabet data, compressed 8 bit data or compressed UCS2 data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

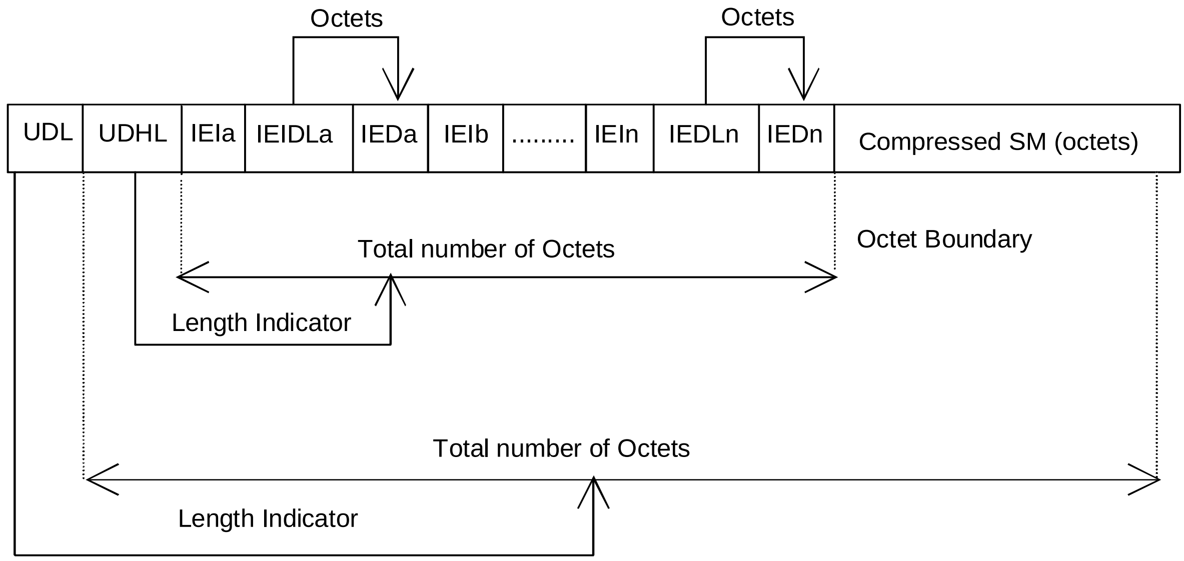

Figure 9.2.3.24 (c)

The definition of the TP-User-Data-Length field which immediately precedes the "Length of User Data Header" is unchanged and shall therefore be the total length of the TP-User-Data field including the Header, if present. (see 9.2.3.16).

The "Length-of-Information-Element" fields shall be the integer representation of the number of octets within its associated "Information-Element-Data" field which follows and shall not include itself in its count value.

The "Length-of-User-Data-Header" field shall be the integer representation of the number of octets within the "User-Data-Header" information fields which follow and shall not include itself in its count or any fill bits which may be present (see text below).

Information Elements may appear in any order and need not follow the order used in the present document. Information Elements are classified into 3 categories as described below.

- SMS Control – identifies those IEIs which have the capability of dictating SMS functionality.
- EMS Control – identifies those IEIs which manage EMS Content IEIs.
- EMS Content – identifies those IEIs containing data of a unique media format.

It is permissible for certain IEs to be repeated within a short message, or within a concatenated message. There is no restriction on the repeatability of IEs in the EMS Content classification. The repeatability of SMS Control and EMS Control IEs is determined on an individual basis. See the IE table below for the repeatability of each IE.

In the event that IEs determined as not repeatable are duplicated, the last occurrence of the IE shall be used. In the event that two or more IEs occur which have mutually exclusive meanings (e.g. an 8bit port address and a 16bit port address), then the last occurring IE shall be used.

If the length of the User Data Header is such that there are too few or too many octets in the final Information Element then the whole User Data Header shall be ignored.

If any reserved values are received within the content of any Information Element then that part of the Information Element shall be ignored.

The support of any Information Element Identifier is optional unless otherwise stated.

The Information Element Identifier octet shall be coded as follows:

VALUE (hex)	MEANING	Classification	Repeatability
00	Concatenated short messages, 8-bit reference number	SMS Control	No
01	Special SMS Message Indication	SMS Control	Yes
02	Reserved	N/A	N/A
03	Value not used to avoid misinterpretation as <LF> character	N/A	N/A
04	Application port addressing scheme, 8 bit address	SMS Control	No
05	Application port addressing scheme, 16 bit address	SMS Control	No
06	SMSC Control Parameters	SMS Control	No
07	UDH Source Indicator	SMS Control	Yes
08	Concatenated short message, 16-bit reference number	SMS Control	No
09	Wireless Control Message Protocol	SMS Control	Note 3
0A	Text Formatting	EMS Control	Yes
0B	Predefined Sound	EMS Content	Yes
0C	User Defined Sound (iMelody max 128 bytes)	EMS Content	Yes
0D	Predefined Animation	EMS Content	Yes
0E	Large Animation (16*16 times 4 = 32*4 =128 bytes)	EMS Content	Yes
0F	Small Animation (8*8 times 4 = 8*4 =32 bytes)	EMS Content	Yes
10	Large Picture (32*32 = 128 bytes)	EMS Content	Yes
11	Small Picture (16*16 = 32 bytes)	EMS Content	Yes
12	Variable Picture	EMS Content	Yes
13	User prompt indicator	EMS Control	Yes
14	Extended Object	EMS Content	Yes
15	Reused Extended Object	EMS Control	Yes
16	Compression Control	EMS Control	No
17	Object Distribution Indicator	EMS Control	Yes
18	Standard WVG object	EMS Content	Yes
19	Character Size WVG object	EMS Content	Yes
1A	Extended Object Data Request Command	EMS Control	No
1B-1F	Reserved for future EMS features (see subclause 3.10)	N/A	N/A
20	RFC 5322 E-Mail Header	SMS Control	No
21	Hyperlink format element	SMS Control	Yes
22	Reply Address Element	SMS Control	No
23	Enhanced Voice Mail Information	SMS Control	No
24	National Language Single Shift	SMS Control	No
25	National Language Locking Shift	SMS Control	No
26 – 6F	Reserved for future use	N/A	N/A
70 – 7F	(U)SIM Toolkit Security Headers	SMS Control	Note 1
80 – 9F	SME to SME specific use	SMS Control	Note 2
A0 – BF	Reserved for future use	N/A	N/A
C0 – DF	SC specific use	SMS Control	Note 2
E0 – FF	Reserved for future use	N/A	N/A
Note 1:	The functionality of these IEIs is defined in 3GPP TSG 31.115 [28], and therefore, the repeatability is not within the scope of this document and will not be determined here.		
Note 2:	The functionality of these IEIs is used in a proprietary fashion by different SMSC vendors, and therefore, are not within the scope of this technical specification.		
Note 3:	The functionality of these IEIs is defined by the WAP Forum and therefore the repeatability is not within the scope of this document and will not be determined here.		

A receiving entity shall ignore (i.e. skip over and commence processing at the next information element) any information element where the IEI is Reserved or not supported. The receiving entity calculates the start of the next information element by looking at the length of the current information element and skipping that number of octets.

The SM itself may be coded as 7, 8 or 16 bit data.

If 7 bit data is used and the TP-UD-Header does not finish on a septet boundary then fill bits are inserted after the last Information Element Data octet up to the next septet boundary so that there is an integral number of septets for the entire TP-UD header. This is to ensure that the SM itself starts on an septet boundary so that an earlier Phase mobile shall be capable of displaying the SM itself although the TP-UD Header in the TP-UD field may not be understood.

It is optional to make the first character of the SM itself a Carriage Return character encoded according to the default 7 bit alphabet so that earlier Phase mobiles, which do not understand the TP-UD-Header, shall over-write the displayed TP-UD-Header with the SM itself.

If 16 bit (USC2) data is used then padding octets are not necessary. The SM itself shall start on an octet boundary.

If 8 bit data is used then padding is not necessary. An earlier Phase mobile shall be able to display the SM itself although the TP-UD header may not be understood.

It is also possible for mobiles not wishing to support the TP-UD header to check the value of the TP-UDHI bit in the SMS-Deliver PDU and the first octet of the TP-UD field and skip to the start of the SM and ignore the TP-UD header.

[TS 23.040, clause 9.2.3.24.1]:

This facility allows short messages to be concatenated to form a longer message.

In the case of uncompressed 8-bit data, the maximum length of the short message within the TP-UD field is 134 (140-6) octets.

In the case of uncompressed GSM 7 bit default alphabet data, the maximum length of the short message within the TP-UD field is 153 (160-7) characters. A character represented by an escape-sequence shall not be split in the middle.

In the case of 16 bit uncompressed USC2 data, the maximum length of the short message within the TP-UD field is 67 ((140-6)/2) characters. A UCS2 character shall not be split in the middle; if the length of the User Data Header is odd, the maximum length of the whole TP-UD field is 139 octets.

In the case of compressed GSM 7 bit default alphabet data, 8 bit data or UCS2 the maximum length of the compressed short message within the TP-UD field is 134 (140-6) octets including the Compression Header and Compression Footer, both or either of which may be present (see clause 3.9).

The maximum length of an uncompressed concatenated short message is 39015 (255*153) default alphabet characters, 34170 (255*134) octets or 17085 (255*67) UCS2 characters.

The maximum length of a compressed concatenated message is 34170 (255*134) octets including the Compression Header and Compression Footer (see clause 3.9 and figure 9.2.3.24.1(a) below).

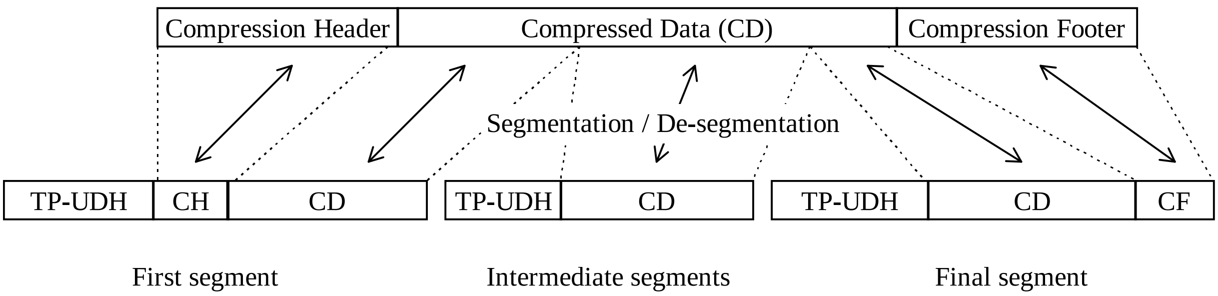

Figure 9.2.3.24.1 (a): Concatenation of a Compressed short message

The Information-Element-Data field contains information set by the application in the SMS-SUBMIT so that the receiving entity is able to re-assemble the short messages in the correct order. Each concatenated short message contains a reference number which together with the originating address and Service Centre address allows the receiving entity to discriminate between concatenated short messages sent from different originating SMEs and/or SCs. In a network which has multiple SCs, it is possible for different segments of a concatenated SM to be sent via different SCs and so it is recommended that the SC address should not be checked by the MS unless the application specifically requires such a check.

The TP elements in the SMS-SUBMIT PDU, apart from TP-MR, TP-SRR, TP-UDL and TP-UD, should remain unchanged for each SM which forms part of a concatenated SM, otherwise this may lead to irrational behaviour. TP-MR must be incremented for every segment of a concatenated message as defined in clause 9.2.3.6. A SC shall handle segments of a concatenated message like any other short message. The relation between segments of a concatenated message is made only at the originator, where the message is segmented, and at the recipient, where the message is reassembled. SMS-COMMANDs identify messages by TP-MR and therefore apply to only one segment of a concatenated message. It is up to the originating SME to issue SMS-COMMANDs for all the required segments of a concatenated message.

The Information-Element-Data octets shall be coded as follows.

Octet 1 Concatenated short message reference number.

This octet shall contain a modulo 256 counter indicating the reference number for a particular concatenated short message. This reference number shall remain constant for every short message which makes up a particular concatenated short message.

Octet 2 Maximum number of short messages in the concatenated short message.

This octet shall contain a value in the range 0 to 255 indicating the total number of short messages within the concatenated short message. The value shall start at 1 and remain constant for every short message which makes up the concatenated short message. If the value is zero then the receiving entity shall ignore the whole Information Element.

Octet 3 Sequence number of the current short message.

This octet shall contain a value in the range 0 to 255 indicating the sequence number of a particular short message within the concatenated short message. The value shall start at 1 and increment by one for every short message sent within the concatenated short message. If the value is zero or the value is greater than the value in octet 2 then the receiving entity shall ignore the whole Information Element.

The IEI and associated IEI length and IEI data shall be present in every segment of the concatenated SM.

[TS 24.341, clause 5.3.1.2]:

When an SM-over-IP sender wants to submit an SM over IP, the SM-over-IP sender shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the PSI of the SC of the SM-over-IP sender;

NOTE 1: The PSI of the SC can be SIP URI or tel URI based on operator policy. The PSI of the SC can be obtained using one of the following methods in the priority order listed below:

1) provided by the user;

2) if UICC is used, then:

- if present in the ISIM, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM of the ISIM as per 3GPP TS 31.103 [18];
- if not present on the ISIM, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM of the USIM as per 3GPP TS 31.102 [19]; or
- if neither present on the ISIM nor on the USIM, then the PSI of the SC contains the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM as per 3GPP TS 31.102 [19]. If the PSI of the SC is based on the E.164 number from the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM then the URI constructed can be either a tel URI or a SIP URI (using the "user=phone" SIP URI parameter format).

3) if SIM is used instead of UICC, then the PSI of the SC contains the TS-Service Centre Address stored in the EF_{SMSP} in DF_TELECOM as per 3GPP TS 51.011 [20]. If the PSI of the SC is based on the E.164 number from the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM then the URI constructed can be either a tel URI or a SIP URI (using the "user=phone" SIP URI parameter format); or

4) if neither the UICC nor SIM is used, then how the PSI of the SC is configured and obtained is through means outside the scope of this specification.

b) the From header, which shall contain a public user identity of the SM-over-IP sender;

NOTE 2: The IP-SM-GW will have to use an address of the SM-over-IP sender that the SC can process (i.e. an E.164 number). This address will come from a tel URI in a P-Asserted-Identity header (as defined in RFC 3325 [13]) placed in the SIP MESSAGE request by the P-CSCF or S-CSCF.

NOTE 3: The SM-over-IP sender has to store the Call-ID of the SIP MESSAGE request, so it can associate the appropriate SIP MESSAGE request including a submit report with it.

c) the To header, which shall contain the SC of the SM-over-IP sender;

d) the Content-Type header, which shall contain "application/vnd.3gpp.sms"; and

e) the body of the request shall contain an RP-DATA message as defined in 3GPP TS 24.011 [8], including the SMS headers and the SMS user information encoded as specified in 3GPP TS 23.040 [3].

NOTE 4: The address of the SC is included in the RP-DATA message content. The address of the SC included in the RP-DATA message content is stored in the EF_{SMSP} in DF_TELECOM of the (U)SIM of the SM-over-IP sender.

NOTE 5: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

NOTE 6: Both the address of the SC and the PSI of the SC can be configured in the $EF_{PSISMSC}$ in DF_TELECOM of the USIM and ISIM respectively using the USAT as per 3GPP TS 31.111 [21].

The SM-over-IP sender may request the SC to return the status of the submitted message. The support of status report capabilities is optional for the SC.

When a SIP MESSAGE request including a submit report in the "vnd.3gpp.sms" payload is received, the SM-over-IP sender shall:

- if SM-over-IP sender supports In-Reply-To header usage and the In-Reply-To header indicates that the request corresponds to a short message submitted by the SM-over-IP sender, generate a 200 (OK) SIP response according to RFC 3428 [14].

  if SM-over-IP sender supports In-Reply-To header usage and the In-Reply-To header indicates that the request does not correspond to a short message submitted by the SM-over-IP sender, a 488 (Not Acceptable here) SIP response according to RFC 3428 [14].

- if SM-over-IP sender does not support In-Reply-To header usage, generate a 200 (OK) SIP response according to RFC 3428 [14]; and extract the payload encoded according to 3GPP TS 24.011 [8] for RP-ACK or RP-ERROR.

Reference(s)

3GPP TS 24.341[90], clauses 5.3.1.2, and TS 23.040 [93], clauses 9.2.3.23, 9.2.3.24 and 9.2.3.24.1.

18.1a.3 Test purpose

1) To verify that the MO UE correctly sends concatenated SMS as described in 3GPP TS 24.341 [90], clauses 5.3.1.2, and TS 23.040 [93], clauses 9.2.3.23, 9.2.3.24 and 9.2.3.24.1.

18.1a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, and registered to IMS services.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

0) Sending of a Mobile Originating Concatenated SMS over IMS is initiated at the UE. The length of SMS text is determined so that the amount of segment of the concatenated SMS is three.

1) The SS waits for the UE to send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the first segment of the concatenated SMS.

2) The SS responds to the SIP MESSAGE request with a 202 Accepted response.

3) The SS sends a SIP MESSAGE request to the UE including a vnd.3gpp.sms payload that contains a short message submission report indicating a positive acknowledgement of the first segment of the concatenated SMS sent by the UE at Step 1).

4) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

5) The SS waits for the UE to send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the second segment of the concatenated SMS.

6) The SS responds to the SIP MESSAGE request with a 202 Accepted response.

7) The SS sends a SIP MESSAGE request to the UE including a vnd.3gpp.sms payload that contains a short message submission report indicating a positive acknowledgement of the second segment of the concatenated SMS sent by the UE at Step 5).

8) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

9) The SS waits for the UE to send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the final segment of the concatenated SMS.

10) The SS responds to the SIP MESSAGE request with a 202 Accepted response.

11) The SS sends a SIP MESSAGE request to the UE including a vnd.3gpp.sms payload that contains a short message submission report indicating a positive acknowledgement of the final segment of the concatenated SMS sent by the UE at Step 9).

12) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
0			Sending of a Mobile Originating Concatenated SMS over IMS is initiated at the UE. The length of SMS text is determined so that the amount of segment of the concatenated SMS is three.	
1	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the first segment of the concatenated SMS.
2	←		202 Accepted	SS responds with 202 Accepted
3	←		SIP MESSAGE request	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the short message submission report indicating a positive acknowledgement of the first segment of the concatenated SMS sent by the UE at Step 1
4	→		200 OK	UE responds with 200 OK
5	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the second segment of the concatenated SMS.
6	←		202 Accepted	SS responds with 202 Accepted
7	←		SIP MESSAGE request	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the short message submission report indicating a positive acknowledgement of the second segment of the concatenated SMS sent by the UE at Step 5
8	→		200 OK	UE responds with 200 OK
9	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the final segment of the concatenated SMS.
10	←		202 Accepted	SS responds with 202 Accepted
11	←		SIP MESSAGE request	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the short message submission report indicating a positive acknowledgement of the final segment of the concatenated SMS sent by the UE at Step 9
12	→		200 OK	UE responds with 200 OK

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable.

Specific Message Contents

SIP MESSAGE request (Step 1)

Use the default message "Message for MO SMS" in Annex A.7.3 with the following exceptions.

Header/param	Cond	Value/remark	Rel	Reference
Message-body		- TP-UDHI='1'B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-MR=any allowed value - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number=any allowed value - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=1		TS 24.011 [92] TS 23.040 [93]

202 Accepted for SIP MESSAGE request (Step 2)

Use the default message “202 Accepted” in annex A.3.3.

SIP MESSAGE request (Step 3)

Use the default message “Short message submission report for MO SMS” in Annex A.7.4

200 OK for SIP MESSAGE request (Step 4)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

SIP MESSAGE request (Step 5)

Use the default message “Message for MO SMS” in Annex A.7.3 with the following exceptions.

Header/param	Cond	Value/remark	Rel	Reference
Message-body		- TP-UDHI=’1’B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-MR= The value sent in the step1 + 1 (incremented) - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number= The same value sent in the step1 - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=2		TS 24.011 [92] TS 23.040 [93]

202 Accepted for SIP MESSAGE request (Step 6)

Use the default message “202 Accepted” in annex A.3.3.

SIP MESSAGE request (Step 7)

Use the default message “Short message submission report for MO SMS” in Annex A.7.4

200 OK for SIP MESSAGE request (Step 8)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

SIP MESSAGE request (Step 9)

Use the default message “Message for MO SMS” in Annex A.7.3 with the following exceptions.

Header/param	Cond	Value/remark	Rel	Reference
Message-body		- TP-UDHI='1'B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-MR= The value sent in the step5 + 1 (incremented) - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number= The same value sent in the step5 - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=3		TS 24.011 [92] TS 23.040 [93]

202 Accepted for SIP MESSAGE request (Step 10)

Use the default message “202 Accepted” in annex A.3.3.

SIP MESSAGE request (Step 11)

Use the default message “Short message submission report for MO SMS” in Annex A.7.4

200 OK for SIP MESSAGE request (Step 12)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

18.1b Mobile Originating SMS / RP-ERROR

18.1b.1 Definition

Test to verify that the UE can successfully receive a RP-ERROR message.

18.1b.2 Conformance requirement

[TS 24.341, clause 5.3.1.1]:

In addition to the procedures specified in subclause 5.3.1, the SM-over-IP sender shall support the procedures specified in 3GPP TS 24.229 [10] appropriate to the functional entity in which the SM-over-IP sender is implemented. The SM-over-IP sender shall build and populate RP-DATA message, containing all the information that a mobile station submitting an SM according to 3GPP TS 24.011 [8] would place, for successful delivery. The SM-over-IP sender shall parse and interpret RP- DATA, RP-ACK and RP-ERROR messages, containing all the information that a mobile station receiving an SM according to 3GPP TS 24.011 [8] would see, in a SM submission or status report.

NOTE 1: If the SM-over-IP sender uses SMR entity timers as specified in 3GPP TS 24.011 [8], then TR1M is set to a value greater than timer F (see 3GPP TS 24.229 [10]).

NOTE 2: If the SM-over-IP sender expects to receive a SM submit report will include the "+g.3gpp.smsip" parameter in the Contact header field when sending a REGISTER request.

[TS 24.341, clause 5.3.1.2]:

When an SM-over-IP sender wants to submit an SM over IP, the SM-over-IP sender shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the PSI of the SC of the SM-over-IP sender;

NOTE 1: The PSI of the SC can be SIP URI or tel URI based on operator policy. The PSI of the SC can be obtained using one of the following methods in the priority order listed below:

1) provided by the user;

2) if UICC is used, then:

- if present in the ISIM, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM of the ISIM as per 3GPP TS 31.103 [18];

- if not present on the ISIM, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM of the USIM as per 3GPP TS 31.102 [19]; or

- if neither present on the ISIM nor on the USIM, then the PSI of the SC contains the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM as per 3GPP TS 31.102 [19]. If the PSI of the SC is based on the E.164 number from the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM then the URI constructed can be either a tel URI or a SIP URI (using the "user=phone" SIP URI parameter format).

3) if SIM is used instead of UICC, then the PSI of the SC contains the TS-Service Centre Address stored in the EF_{SMSP} in DF_TELECOM as per 3GPP TS 51.011 [20]. If the PSI of the SC is based on the E.164 number from the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM then the URI constructed can be either a tel URI or a SIP URI (using the "user=phone" SIP URI parameter format); or

4) if neither the UICC nor SIM is used, then how the PSI of the SC is configured and obtained is through means outside the scope of this specification.

b) the From header, which shall contain a public user identity of the SM-over-IP sender;

NOTE 2: The IP-SM-GW will have to use an address of the SM-over-IP sender that the SC can process (i.e. an E.164 number). This address will come from a tel URI in a P-Asserted-Identity header (as defined in RFC 3325 [13]) placed in the SIP MESSAGE request by the P-CSCF or S-CSCF.

NOTE 3: The SM-over-IP sender has to store the Call-ID of the SIP MESSAGE request, so it can associate the appropriate SIP MESSAGE request including a submit report with it.

c) the To header, which shall contain the SC of the SM-over-IP sender;

d) the Content-Type header, which shall contain "application/vnd.3gpp.sms"; and

e) the body of the request shall contain an RP-DATA message as defined in 3GPP TS 24.011 [8], including the SMS headers and the SMS user information encoded as specified in 3GPP TS 23.040 [3].

NOTE 4: The address of the SC is included in the RP-DATA message content. The address of the SC included in the RP-DATA message content is stored in the EF_{SMSP} in DF_TELECOM of the (U)SIM of the SM-over-IP sender.

NOTE 5: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

NOTE 6: Both the address of the SC and the PSI of the SC can be configured in the $EF_{PSISMSC}$ in DF_TELECOM of the USIM and ISIM respectively using the USAT as per 3GPP TS 31.111 [21].

The SM-over-IP sender may request the SC to return the status of the submitted message. The support of status report capabilities is optional for the SC.

When a SIP MESSAGE request including a submit report in the "vnd.3gpp.sms" payload is received, the SM-over-IP sender shall:

- if SM-over-IP sender supports In-Reply-To header usage and the In-Reply-To header indicates that the request corresponds to a short message submitted by the SM-over-IP sender, generate a 200 (OK) SIP response according to RFC 3428 [14].

  if SM-over-IP sender supports In-Reply-To header usage and the In-Reply-To header indicates that the request does not correspond to a short message submitted by the SM-over-IP sender, a 488 (Not Acceptable here) SIP response according to RFC 3428 [14].

- if SM-over-IP sender does not support In-Reply-To header usage, generate a 200 (OK) SIP response according to RFC 3428 [14]; and extract the payload encoded according to 3GPP TS 24.011 [8] for RP-ACK or RP-ERROR.

[TS 24.341 clause 5.3.1.3]:

When a SIP MESSAGE request including a status report in the "vnd.3gpp.sms" payload is delivered, the SM-over-IP sender shall:

- generate a SIP response according to RFC 3428 [14];
- extract the payload encoded according to 3GPP TS 24.011 [8] for RP-DATA; and
- create a delivery report for the status report as described in subclause 5.3.2.4. The content of the delivery report is defined in 3GPP TS 24.011 [8].

[TS 24.341 clause 5.3.2.4]:

When an SM-over-IP receiver wants to send an SM delivery report over IP, the SM-over-IP receiver shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the IP-SM-GW;

NOTE 1: The address of the IP-SM-GW is received in the P-Asserted-Identity header in the SIP MESSAGE request including the delivered short message.

b) the From header, which shall contain a public user identity of the SM-over-IP receiver.

c) the To header, which shall contain the IP-SM-GW;

b) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

c) the body of the request shall contain the RP-ACK or RP-ERROR message for the SM delivery report, as defined in 3GPP TS 24.011 [8].

NOTE 2: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

[TS 24.011 clause 8.2.5.4]:

This element is a variable length element always included in the RP-ERROR message, conveying a negative result of a RP-DATA message transfer attempt or RP-SMMA notification attempt. The element contains a cause value and optionally a diagnostic field giving further details of the error cause.

The coding of the cause value is given in table 8.4/3GPP TS 24.011. The mapping between error causes in 3GPP TS 24.011 and 3GPP TS 29.002 (MAP) is specified in 3GPP TS 23.040. Parameters included in the return error from MAP (e.g. System Failure) are mapped directly into the diagnostic field.

8 7 6 5 4 3 2 1		
0	1 0 0 0 0 1 0 RP-Cause IEI	1 octet
Length indicator		1 octet
0 ext	Cause value Cause value	1 octet
Diagnostic field		1 octet *

Figure 8.8/3GPP TS 24.011: RP-Cause element layout

Table 8.4/3GPP TS 24.011 (part 1): Cause values that may be contained in an RP-ERROR message in a mobile originating SM-transfer attempt

Cause value Class value	Cause number	Cause
7 6 5 4 3 2 1	#	
0 0 0 0 0 0 1	1	Unassigned (unallocated) number
0 0 0 1 0 0 0	8	Operator determined barring
0 0 0 1 0 1 0	10	Call barred
0 0 0 1 0 1 1	11	Reserved
0 0 1 0 1 0 1	21	Short message transfer rejected
0 0 1 1 0 1 1	27	Destination out of order
0 0 1 1 1 0 0	28	Unidentified subscriber
0 0 1 1 1 0 1	29	Facility rejected
0 0 1 1 1 1 0	30	Unknown subscriber
0 1 0 0 1 1 0	38	Network out of order
0 1 0 1 0 0 1	41	Temporary failure
0 1 0 1 0 1 0	42	Congestion
0 1 0 1 1 1 1	47	Resources unavailable, unspecified
0 1 1 0 0 1 0	50	Requested facility not subscribed
1 0 0 0 1 0 1	69	Requested facility not implemented
1 0 1 0 0 0 1	81	Invalid short message transfer reference value
1 0 1 1 1 1 1	95	Semantically incorrect message
1 1 0 0 0 0 0	96	Invalid mandatory information
1 1 0 0 0 0 1	97	Message type non-existent or not implemented
1 1 0 0 0 1 0	98	Message not compatible with short message protocol state
1 1 0 0 0 1 1	99	Information element non-existent or not implemented
1 1 0 1 1 1 1	111	Protocol error, unspecified
1 1 1 1 1 1 1	127	Interworking, unspecified
All other cause values shall be treated as cause number 41, "Temporary Failure".		

Reference(s)

3GPP TS 24.341[90], clauses 5.3.1.1, 5.3.1.2, 5.3.1.3 and 5.3.2.4, and TS 24.011 [92], clause 8.2.5.4.

18.1b.3 Test purpose

1) To verify that when sending of a Mobile Originating SMS over IMS is initiated, the UE sends a SIP MESSAGE request constructed as described in 3GPP TS 24.341 [90], clause 5.3.1.2; and

2) To verify that the UE correctly handles reception of a SIP MESSAGE request indicating RP-ERROR.

18.1b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, and registered to IMS services.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

1) Sending of a Mobile Originating SMS over IMS is initiated at the UE. The SS waits for the UE to send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the short message.

2) The SS responds to the SIP MESSAGE request with a 202 Accepted response.

3) The SS sends a SIP MESSAGE request to the UE including a vnd.3gpp.sms payload and RP-ERROR message.

4) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a short message
2	←		202 Accepted	SS responds with 202 Accepted
3	←		SIP MESSAGE request	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload and RP-ERROR message
4	→		200 OK	UE responds with 200 OK

NOTE: The default messages contents in annex A are used with condition “IMS security” or “GIBA” when applicable

Specific Message Contents

SIP MESSAGE request (Step 1)

Use the default message “Message for MO SMS” in Annex A.7.3

202 Accepted for SIP MESSAGE request (Step 2)

Use the default message “202 Accepted” in annex A.3.3.

SIP MESSAGE request (Step 3)

Use the default message “Short message submission report for MO SMS” in Annex A.7.4 with the following exception.

Header/param	Cond	Value/remark	Rel	Reference
Message-body		RP-ERROR message with RP-Cause Data: Length: 2, Length indicator = 1 Extension: not extended Cause value: 38 (Network out of order)		TS 24.011 [92] TS 23.040 [93]

200 OK for SIP MESSAGE request (Step 4)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

18.2 Mobile Terminating SMS

18.2.1 Definition

Test to verify that the UE correctly implemented the role of an SM-over-IP receiver.

18.2.2 Conformance requirement

[TS 24.341, clause 5.3.2.3]

When a SIP MESSAGE request including a short message in the "vnd.3gpp.sms" payload is delivered, the SM-over-IP receiver shall:

- generate a SIP response according to RFC 3428;
- extract the payload encoded according to 3GPP TS 24.011 for RP-DATA; and
- create a delivery report as described in subclause 5.3.2.4. The content of the report is defined in 3GPP TS 24.011.

[TS 24.341, clause 5.3.2.4]

When an SM-over-IP receiver wants to send an SM delivery report over IP, the SM-over-IP receiver shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the IP-SM-GW;

NOTE 1: The address of the IP-SM-GW is received in the P-Asserted-Identity header in the SIP MESSAGE request including the delivered short message.

b) the From header, which shall contain a public user identity of the SM-over-IP receiver.

c) the To header, which shall contain the IP-SM-GW;

b) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

c) the body of the request shall contain the RP-ACK or RP-ERROR message for the SM delivery report, as defined in 3GPP TS 24.011 [8].

NOTE 2: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

Reference(s)

3GPP TS 24.341[90], clause 5.3.2.3 and 5.3.2.4.

18.2.3 Test purpose

1) To verify that the UE performs correct exchange of SIP protocol signalling messages when an SM is received.
2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.
3) To verify that within SIP signalling the UE performs the correct exchange of message body.

18.2.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

1) SS sends a Short Message included in the message-body of MESSAGE.

2) UE responds with a 200 OK.

3) When the payload is extracted, the UE responds with a delivery report included in the message-body of MESSAGE.

4) SS responds with a 202 ACCEPTED.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		MESSAGE	The SS sends a Short Message.
2	→		200 OK	The UE responds with 200 OK.
3	→		MESSAGE	The UE responds with a delivery report.
4	←		202 ACCEPTED	The SS sends an accepted response.

Specific Message Contents

MESSAGE (Step 1)

Use the default message "MESSAGE for MT SMS" in annex A.7.1.

200 OK (Step 2)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with condition A5 "Any response sent by the UE within a dialog".

MESSAGE (Step 3)

Use the default message "MESSAGE for delivery report" in annex A.7.2.

202 ACCEPTED (Step 4)

Use the default message "202 ACCEPTED" in annex A.3.3

18.2.5 Test requirements

The UE shall send requests and responses as described in clause 18.2.4.

18.2a Mobile Terminating Concatenated SMS

18.2a.1 Definition

Test to verify that the UE is able to receive a Mobile Terminating Concatenated SMS over IMS correctly. This process is described in 3GPP TS 23.040 [93], clauses 9.2.3.23, 9.2.3.24 and 9.2.3.24.1 and TS 24.341 [90], clauses 5.3.1.2 .

18.2a.2 Conformance requirement

[TS 23.040, clause 9.2.3.23]:

The TP-User-Data-Header-Indicator is a 1 bit field within bit 6 of the first octet of the following six PDUs:

- SMS-SUBMIT,
- SMS-SUBMIT-REPORT,
- SMS-DELIVER,
- SMS-DELIVER-REPORT,

- SMS-STATUS-REPORT,
- SMS-COMMAND.

TP-UDHI has the following values.

Bit no. 6 0 The TP-UD field contains only the short message

1 The beginning of the TP-UD field contains a Header in addition to the short message.

[TS 23.040, clause 9.2.3.24]:

The length of the TP-User-Data field is defined in the PDU's of the SM-TL (see clause 9.2.2).

The TP-User-Data field may comprise just the short message itself or a Header in addition to the short message depending upon the setting of TP-UDHI.

Where the TP-UDHI value is set to 0 the TP-User-Data field comprises the short message only, where the user data can be 7 bit (default alphabet) data, 8 bit data, or 16 bit (UCS2 [24]) data.

Where the TP-UDHI value is set to 1 the first octets of the TP-User-Data field contains a Header in the following order starting at the first octet of the TP-User-Data field.

Irrespective of whether any part of the User Data Header is ignored or discarded, the MS shall always store the entire TPDU exactly as received.

FIELD	LENGTH
Length of User Data Header	1 octet
Information-Element-Identifier "A"	1 octet
Length of Information-Element "A"	1 octet
Information-Element "A" Data	0 to "n" octets
Information-Element-Identifier "B"	1 octet
Length of Information-Element "B"	1 octet
Information-Element "B" Data	0 to "n" octets
Information-Element-Identifier "X"	1 octet
Length of Information-Element "X"	1 octet
Information-Element "X" Data	0 to "n" octets

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for uncompressed GSM 7 bit default alphabet data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

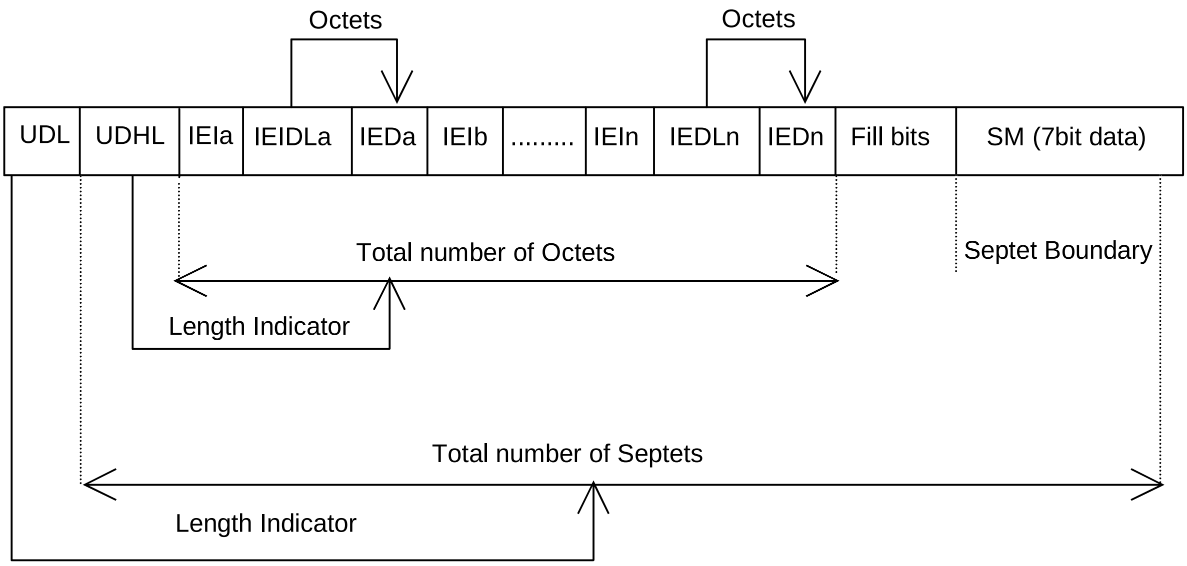

Figure 9.2.3.24 (a)

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for uncompressed 8 bit data or uncompressed UCS2 data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

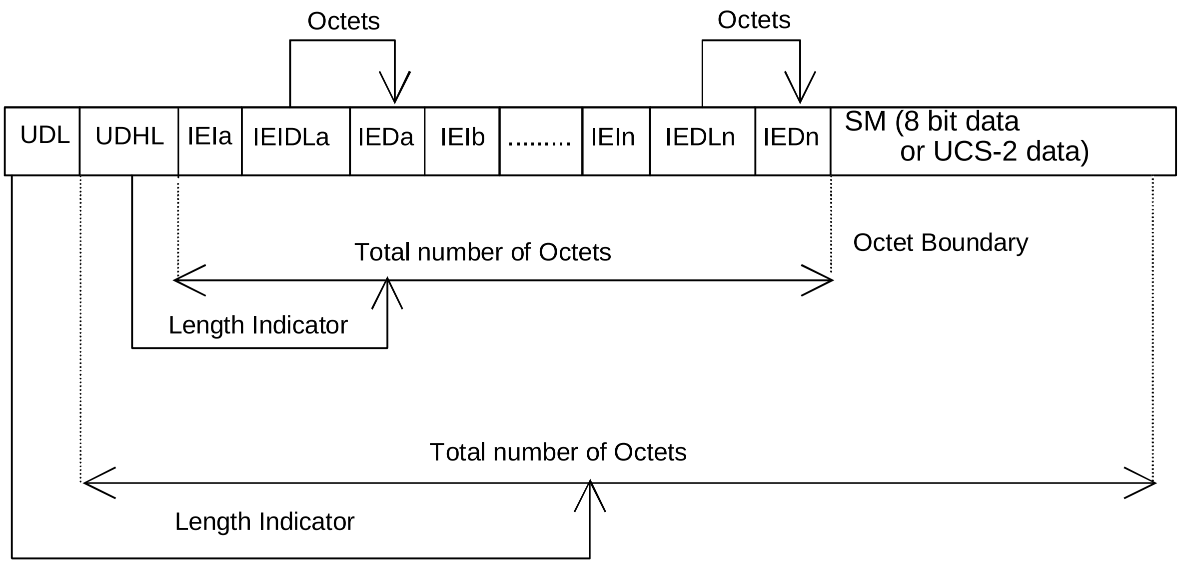

Figure 9.2.3.24 (b)

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for compressed GSM 7 bit default alphabet data, compressed 8 bit data or compressed UCS2 data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

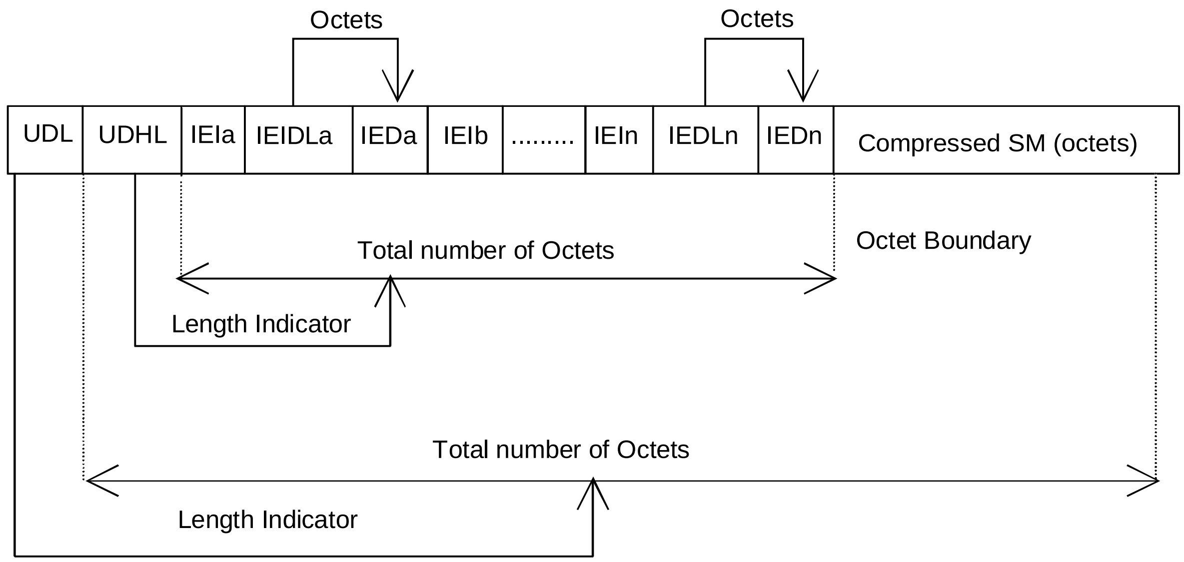

Figure 9.2.3.24 (c)

The definition of the TP-User-Data-Length field which immediately precedes the "Length of User Data Header" is unchanged and shall therefore be the total length of the TP-User-Data field including the Header, if present. (see 9.2.3.16).

The "Length-of-Information-Element" fields shall be the integer representation of the number of octets within its associated "Information-Element-Data" field which follows and shall not include itself in its count value.

The "Length-of-User-Data-Header" field shall be the integer representation of the number of octets within the "User-Data-Header" information fields which follow and shall not include itself in its count or any fill bits which may be present (see text below).

Information Elements may appear in any order and need not follow the order used in the present document. Information Elements are classified into 3 categories as described below.

- SMS Control – identifies those IEIs which have the capability of dictating SMS functionality.
- EMS Control – identifies those IEIs which manage EMS Content IEIs.
- EMS Content – identifies those IEIs containing data of a unique media format.

It is permissible for certain IEs to be repeated within a short message, or within a concatenated message. There is no restriction on the repeatability of IEs in the EMS Content classification. The repeatability of SMS Control and EMS Control IEs is determined on an individual basis. See the IE table below for the repeatability of each IE.

In the event that IEs determined as not repeatable are duplicated, the last occurrence of the IE shall be used. In the event that two or more IEs occur which have mutually exclusive meanings (e.g. an 8bit port address and a 16bit port address), then the last occurring IE shall be used.

If the length of the User Data Header is such that there are too few or too many octets in the final Information Element then the whole User Data Header shall be ignored.

If any reserved values are received within the content of any Information Element then that part of the Information Element shall be ignored.

The support of any Information Element Identifier is optional unless otherwise stated.

The Information Element Identifier octet shall be coded as follows:

VALUE (hex)	MEANING	Classification	Repeatability
00	Concatenated short messages, 8-bit reference number	SMS Control	No
01	Special SMS Message Indication	SMS Control	Yes
02	Reserved	N/A	N/A
03	Value not used to avoid misinterpretation as <LF> character	N/A	N/A
04	Application port addressing scheme, 8 bit address	SMS Control	No
05	Application port addressing scheme, 16 bit address	SMS Control	No
06	SMSC Control Parameters	SMS Control	No
07	UDH Source Indicator	SMS Control	Yes
08	Concatenated short message, 16-bit reference number	SMS Control	No
09	Wireless Control Message Protocol	SMS Control	Note 3
0A	Text Formatting	EMS Control	Yes
0B	Predefined Sound	EMS Content	Yes
0C	User Defined Sound (iMelody max 128 bytes)	EMS Content	Yes
0D	Predefined Animation	EMS Content	Yes
0E	Large Animation (16*16 times 4 = 32*4 =128 bytes)	EMS Content	Yes
0F	Small Animation (8*8 times 4 = 8*4 =32 bytes)	EMS Content	Yes
10	Large Picture (32*32 = 128 bytes)	EMS Content	Yes
11	Small Picture (16*16 = 32 bytes)	EMS Content	Yes
12	Variable Picture	EMS Content	Yes
13	User prompt indicator	EMS Control	Yes
14	Extended Object	EMS Content	Yes
15	Reused Extended Object	EMS Control	Yes
16	Compression Control	EMS Control	No
17	Object Distribution Indicator	EMS Control	Yes
18	Standard WVG object	EMS Content	Yes
19	Character Size WVG object	EMS Content	Yes
1A	Extended Object Data Request Command	EMS Control	No
1B-1F	Reserved for future EMS features (see subclause 3.10)	N/A	N/A
20	RFC 5322 E-Mail Header	SMS Control	No
21	Hyperlink format element	SMS Control	Yes
22	Reply Address Element	SMS Control	No
23	Enhanced Voice Mail Information	SMS Control	No
24	National Language Single Shift	SMS Control	No
25	National Language Locking Shift	SMS Control	No
26 – 6F	Reserved for future use	N/A	N/A
70 – 7F	(U)SIM Toolkit Security Headers	SMS Control	Note 1
80 – 9F	SME to SME specific use	SMS Control	Note 2
A0 – BF	Reserved for future use	N/A	N/A
C0 – DF	SC specific use	SMS Control	Note 2
E0 – FF	Reserved for future use	N/A	N/A
Note 1: The functionality of these IEIs is defined in 3GPP TSG 31.115 [28], and therefore, the repeatability is not within the scope of this document and will not be determined here. Note 2: The functionality of these IEIs is used in a proprietary fashion by different SMSC vendors, and therefore, are not within the scope of this technical specification. Note 3: The functionality of these IEIs is defined by the WAP Forum and therefore the repeatability is not within the scope of this document and will not be determined here.			

A receiving entity shall ignore (i.e. skip over and commence processing at the next information element) any information element where the IEI is Reserved or not supported. The receiving entity calculates the start of the next information element by looking at the length of the current information element and skipping that number of octets.

The SM itself may be coded as 7, 8 or 16 bit data.

If 7 bit data is used and the TP-UD-Header does not finish on a septet boundary then fill bits are inserted after the last Information Element Data octet up to the next septet boundary so that there is an integral number of septets for the entire TP-UD header. This is to ensure that the SM itself starts on an septet boundary so that an earlier Phase mobile shall be capable of displaying the SM itself although the TP-UD Header in the TP-UD field may not be understood.

It is optional to make the first character of the SM itself a Carriage Return character encoded according to the default 7 bit alphabet so that earlier Phase mobiles, which do not understand the TP-UD-Header, shall over-write the displayed TP-UD-Header with the SM itself.

If 16 bit (USC2) data is used then padding octets are not necessary. The SM itself shall start on an octet boundary.

If 8 bit data is used then padding is not necessary. An earlier Phase mobile shall be able to display the SM itself although the TP-UD header may not be understood.

It is also possible for mobiles not wishing to support the TP-UD header to check the value of the TP-UDHI bit in the SMS-Deliver PDU and the first octet of the TP-UD field and skip to the start of the SM and ignore the TP-UD header.

[TS 23.040, clause 9.2.3.24.1]:

This facility allows short messages to be concatenated to form a longer message.

In the case of uncompressed 8-bit data, the maximum length of the short message within the TP-UD field is 134 (140-6) octets.

In the case of uncompressed GSM 7 bit default alphabet data, the maximum length of the short message within the TP-UD field is 153 (160-7) characters. A character represented by an escape-sequence shall not be split in the middle.

In the case of 16 bit uncompressed USC2 data, the maximum length of the short message within the TP-UD field is 67 ((140-6)/2) characters. A UCS2 character shall not be split in the middle; if the length of the User Data Header is odd, the maximum length of the whole TP-UD field is 139 octets.

In the case of compressed GSM 7 bit default alphabet data, 8 bit data or UCS2 the maximum length of the compressed short message within the TP-UD field is 134 (140-6) octets including the Compression Header and Compression Footer, both or either of which may be present (see clause 3.9).

The maximum length of an uncompressed concatenated short message is 39015 (255*153) default alphabet characters, 34170 (255*134) octets or 17085 (255*67) UCS2 characters.

The maximum length of a compressed concatenated message is 34170 (255*134) octets including the Compression Header and Compression Footer (see clause 3.9 and figure 9.2.3.24.1(a) below).

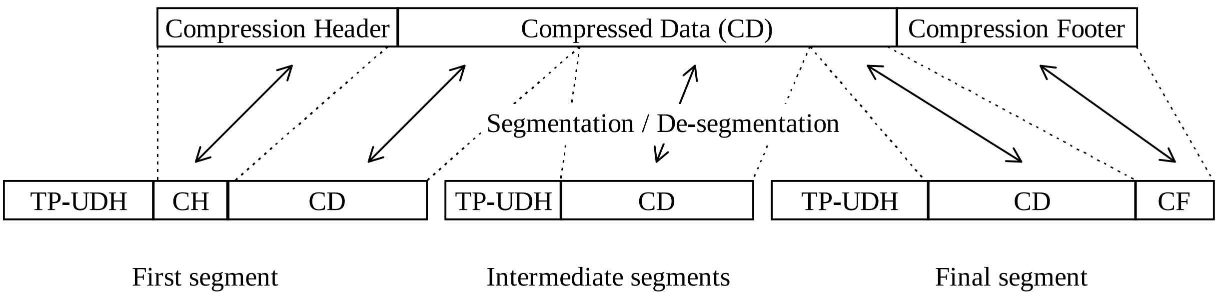

Figure 9.2.3.24.1 (a): Concatenation of a Compressed short message

The Information-Element-Data field contains information set by the application in the SMS-SUBMIT so that the receiving entity is able to re-assemble the short messages in the correct order. Each concatenated short message contains a reference number which together with the originating address and Service Centre address allows the receiving entity to discriminate between concatenated short messages sent from different originating SMEs and/or SCs. In a network which has multiple SCs, it is possible for different segments of a concatenated SM to be sent via different SCs and so it is recommended that the SC address should not be checked by the MS unless the application specifically requires such a check.

The TP elements in the SMS-SUBMIT PDU, apart from TP-MR, TP-SRR, TP-UDL and TP-UD, should remain unchanged for each SM which forms part of a concatenated SM, otherwise this may lead to irrational behaviour. TP-MR must be incremented for every segment of a concatenated message as defined in clause 9.2.3.6. A SC shall handle segments of a concatenated message like any other short message. The relation between segments of a concatenated message is made only at the originator, where the message is segmented, and at the recipient, where the message is reassembled. SMS-COMMANDs identify messages by TP-MR and therefore apply to only one segment of a concatenated message. It is up to the originating SME to issue SMS-COMMANDs for all the required segments of a concatenated message.

The Information-Element-Data octets shall be coded as follows.

Octet 1 Concatenated short message reference number.

This octet shall contain a modulo 256 counter indicating the reference number for a particular concatenated short message. This reference number shall remain constant for every short message which makes up a particular concatenated short message.

Octet 2 Maximum number of short messages in the concatenated short message.

This octet shall contain a value in the range 0 to 255 indicating the total number of short messages within the concatenated short message. The value shall start at 1 and remain constant for every short message which makes up the concatenated short message. If the value is zero then the receiving entity shall ignore the whole Information Element.

Octet 3 Sequence number of the current short message.

This octet shall contain a value in the range 0 to 255 indicating the sequence number of a particular short message within the concatenated short message. The value shall start at 1 and increment by one for every short message sent within the concatenated short message. If the value is zero or the value is greater than the value in octet 2 then the receiving entity shall ignore the whole Information Element.

The IEI and associated IEI length and IEI data shall be present in every segment of the concatenated SM.

[TS 24.341, clause 5.3.2.3]

When a SIP MESSAGE request including a short message in the "vnd.3gpp.sms" payload is delivered, the SM-over-IP receiver shall:

- generate a SIP response according to RFC 3428;
- extract the payload encoded according to 3GPP TS 24.011 for RP-DATA; and
- create a delivery report as described in subclause 5.3.2.4. The content of the report is defined in 3GPP TS 24.011.

[TS 24.341, clause 5.3.2.4]

When an SM-over-IP receiver wants to send an SM delivery report over IP, the SM-over-IP receiver shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the IP-SM-GW;

NOTE 1: The address of the IP-SM-GW is received in the P-Asserted-Identity header in the SIP MESSAGE request including the delivered short message.

b) the From header, which shall contain a public user identity of the SM-over-IP receiver.

c) the To header, which shall contain the IP-SM-GW;

b) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

c) the body of the request shall contain the RP-ACK or RP-ERROR message for the SM delivery report, as defined in 3GPP TS 24.011 [8].

NOTE 2: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

Reference(s)

3GPP TS 24.341 [90], clauses 5.3.2.3 and 5.3.2.4, and TS 23.040 [93], clauses 9.2.3.23, 9.2.3.24 and 9.2.3.24.1.

18.2a.3 Test purpose

1) To verify that the UE performs correct exchange of SIP protocol signalling messages when an concatenated SM is received.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of message body.

18.2a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, and registered to IMS services.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

1) SS sends a first segment of a concatenated SMS in the message-body of SIP_MESSAGE.

2) UE responds with a 200 OK.

3) When the payload is extracted, the UE responds with a delivery report included in the message-body of MESSAGE.

4) SS responds with a 202 ACCEPTED.

5) SS sends a second segment of a concatenated SMS in the message-body of SIP_MESSAGE.

6) The UE responds with a 200 OK.

7) When the payload is extracted, the UE responds with a delivery report included in the message-body of MESSAGE.

8) SS responds with a 202 ACCEPTED.

9) SS sends a fnal segment of a concatenated SMS in the message-body of SIP_MESSAGE.

10) The UE responds with a 200 OK.

11) When the payload is extracted, the UE responds with a delivery report included in the message-body of MESSAGE.

12) SS responds with a 202 ACCEPTED.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		SIP MESSAGE request	SS sends a first segment of a concatenated SMS in the message-body of SIP MESSAGE
2	→		200 OK	UE responds with 200 OK
3	→		SIP MESSAGE request	UE responds with a delivery report included in the message-body of MESSAGE
4	←		202 Accepted	SS responds with 202 Accepted
5	←		SIP MESSAGE request	SS sends a second segment of a concatenated SMS in the message-body of SIP MESSAGE
6	→		200 OK	UE responds with 200 OK
7	→		SIP MESSAGE request	UE responds with a delivery report included in the message-body of MESSAGE
8	←		202 Accepted	SS responds with 202 Accepted
9	←		SIP MESSAGE request	SS sends a final segment of a concatenated SMS in the message-body of SIP MESSAGE
10	→		200 OK	UE responds with 200 OK
11	→		SIP MESSAGE request	UE responds with a delivery report included in the message-body of MESSAGE
12	←		202 Accepted	SS responds with 202 Accepted

Specific Message Contents

SIP MESSAGE request (Step 1)

Use the default message “MESSAGE for MT SMS” in annex A.7.1 with the following exceptions.

Header/param	Cond	Value/remark	Rel	Reference
Message-body		- TP-RP=’0’B (TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER) - TP-MMS=’0’B (More messages are waiting for the MS in this SC) - TP-UDHI=’1’B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-PID=’00000000’B - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number=any allowed value - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=1		TS 24.011 [92] TS 23.040 [93]

200 OK (Step 2)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with condition A5 “Any response sent by the UE within a dialog”.

SIP MESSAGE (Step 3)

Use the default message “MESSAGE for delivery report” in annex A.7.2.

202 ACCEPTED (Step 4)

Use the default message “202 ACCEPTED” in annex A.3.3

SIP MESSAGE request (Step 5)

Use the default message “MESSAGE for MT SMS” in annex A.7.1 with the following exceptions.

Header/param	Cond	Value/remark	Rel	Reference
Message-body		- TP-RP=’0’B (TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER) - TP-MMS=’0’B (More messages are waiting for the MS in this SC) - TP-UDHI=’1’B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-PID=’00000000’B - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number=The same value sent in the step1 - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=2		TS 24.011 [92] TS 23.040 [93]

200 OK (Step 6)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with condition A5 “Any response sent by the UE within a dialog”.

SIP MESSAGE (Step 7)

Use the default message “MESSAGE for delivery report” in annex A.7.2.

202 ACCEPTED (Step 8)

Use the default message “202 ACCEPTED” in annex A.3.3

SIP MESSAGE request (Step 9)

Use the default message “MESSAGE for MT SMS” in annex A.7.1 with the following exceptions.

Header/param	Cond	Value/remark	Rel	Reference
Message-body		- TP-RP=’0’B (TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER) - TP-MMS=’1’B (No more messages are waiting for the MS in this SC) - TP-UDHI=’1’B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-PID=’00000000’B - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number=The same value sent in the step5 - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=3		TS 24.011 [92] TS 23.040 [93]

200 OK (Step 10)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with condition A5 “Any response sent by the UE within a dialog”.

SIP MESSAGE (Step 11)

Use the default message “MESSAGE for delivery report” in annex A.7.2.

202 ACCEPTED (Step 12)

Use the default message “202 ACCEPTED” in annex A.3.3

19 Emergency Service over IMS

19.1 Emergency session set-up within an emergency registration

19.1.1 Emergency call with emergency registration / Success / Location information available

19.1.1.1 Definition

Test to verify that the UE can correctly register to IMS emergency services and initiate an IMS emergency call when UE is registered to IMS non-emergency services of the HPLMN either with ISIM or USIM. The process consists of setting up EPS emergency bearers, sending initial emergency registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally initiating the emergency call.

19.1.1.2 Conformance requirement

[TS 24.229 clause 4.7]:

A number of mechanisms also exist for providing location in support of emergency calls, both for routeing to a PSAP, and for use by the PSAP itself, in the IM CN subsystem:

a) by the inclusion by the UE of the Geolocation header field containing a location by reference or by value (see RFC 6442 [98]);

b) by the inclusion by the UE of a P-Access-Network-Info header field, which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;

c) by the inclusion by the P-CSCF of a P-Access-Network-Info header field based on information supplied by either the PCRF or the NASS, and which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;

d) by the allocation of a location reference that relates to the call by the LRF. Location is then supplied to the recipient over the Le interface (see 3GPP TS 23.167 [4B] for a definition of the Le interface) along with other call information. The LRF can obtain the location from entities outside the IM CN subsystem, e.g. by the e2 interface from the NASS (see ETSI TS 283 035) or from the Gateway Mobile Location Centre (GMLC).

...

Which means of providing location is used depends on local regulatory and operator requirements. One or more mechanisms can be used. Location can be subject to privacy constraints.

A number of mechanisms also exist for providing location in support of emergency calls, both for routeing to a PSAP, and for use by the PSAP itself, in the IM CN subsystem:

a) by the inclusion by the UE of the Geolocation header field containing a location by reference or by value (see RFC 6442 [89]);

b) by the inclusion by the UE of a P-Access-Network-Info header field, which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;

c) by the inclusion by the P-CSCF of a P-Access-Network-Info header field based on information supplied by either the PCRF or the NASS, and which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;

d) by the allocation of a location reference that relates to the call by the LRF. Location is then supplied to the recipient over the Le interface (see 3GPP TS 23.167 [4B] for a definition of the Le interface) along with other call information. The LRF can obtain the location from entities outside the IM CN subsystem, e.g. by the e2 interface from the NASS (see ETSI TS 283 035 [98] or from the Gateway Mobile Location Centre (GMLC).

…

Which means of providing location is used depends on local regulatory and operator requirements. One or more mechanisms can be used. Location can be subject to privacy constraints.

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 and 3GPP TS 23.167 to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

...

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

- the first entry in the list of public user identities provisioned in the UE;
- the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and
- the derived temporary public user identity, in all other cases.

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a Request-URI in the INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031. An additional sub-service type can be added if information on the type of emergency service is known;

3) the UE shall insert in the INVITE request, a To header field with:

- the same emergency service URN as in the Request-URI; or

- if the UE cannot perform local dialstring interpretation for the dialled digits, a dialstring URI representing the dialled digits in accordance with RFC 4967 or a tel URL representing the dialled digits;

NOTE 1: This version of this document does not provide any specified handling of a URI with the dialled digits in accordance with RFC 4967 at an entity within the IM CN subsystem. Behaviour when this is used is therefore not defined.

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 3: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, then the UE shall include its location information in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, and set the Geolocation-Routing header field to "yes", all in accordance with RFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 and include the location object in a message body with the content type application/pidf+xml with RFC 6442 [98]. The Geolocation header field is set to a Content ID, set the Geolocation-Routing header field to "yes", all in accordance with RFC 6442 [98]; and

NOTE 4: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

8) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 5: RFC 3261 provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

- if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

[TS 24.229 annex L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

...

When activating a EPS bearer context to perform emergency registration, the UE shall request a PDN connection for emergency bearer services as described in 3GPP TS 24.301. The procedures for EPS bearer context activation and P-CSCF discovery, as described in subclause L.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 will be considered as a visited network.

[TS 24.237 clause 7.2]:

When originating an emergency call as specified in 3GPP TS 24.229 and if the SC UE has an IMEI, then the SC UE shall include the instance-id media feature tag as specified in IETF RFC 5626 with value based on the IMEI as defined in 3GPP TS 23.003 in the Contact header field of the SIP INVITE request.

[TS 23.003 clause 13.8]:

An instance-id is a SIP Contact header parameter that uniquely identifies the SIP UA performing a registration.

When an IMEI is available, the instance-id shall take the form of a IMEI URN (see RFC 7254 [122]). The format of the instance-id shall take the form "urn:gsma:imei:<gsma-specifier-defined-substring>" where by the gsma-specifier-defined-substring shall be the IMEI encoded as defined in RFC 7254 [122]. The optional <gsma-specifier-defined-param> parameters shall not be included in the instance-id. An example of such an instance-id is as follows:

EXAMPLE: urn:gsma:imei:90420156-025763-0

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.3 and Annex L2.2.6, TS 24.237 [110] clause 7.2 and TS 23.003 [32] clause 13.8 (release 9)

19.1.1.3 Test purpose

1) To verify that the UE is able to request activation of EPS emergency bearer contexts, according to 3GPP TS 24.229 [10] annex L.2.2.6; and

2) To verify that the UE sends a correctly composed initial SIP REGISTER request for emergency services to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.6.1; and

3) To verify that the UE is able to use the IMS security procedures for the IMS emergency registration, as defined for IMS AKA and IPSec within 3GPP TS 24.229 [10] clause 5.1.1; and

4) To verify the support of the UE for providing its location within the IMS emergency call signalling messages, as defined within 3GPP TS 24.229 [10] clause 5.1.6.8.3; and

5) To verify that the UI sends a correctly composed SIP INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.3 and 6.1.2.

19.1.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test environment shall be set up to provide the needed input to the UE, in order for the UE to derive its location, if the UE uses Geolocation header for providing its geographical location. This shall be done by use of the test function Update UE Location Information defined in TS 34.109 [117] or in TS 36.509 [118] depending on the RAT being used in the test case, if supported by the UE according to pc_UpdateUE_LocationInformation. Otherwise, or in addition any other suitable method may also be used.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call.

16) Call is released on the UE using C.32 procedure.

17) Void

18) Emergency Bearer context is deactivated

Expected sequence:

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
16-16A4	→		Steps defined in annex C.32	The UE releases the call
17			Void	
18			EPS emergency bearer context deactivation by the SS.	EPS Bearer Deactivation procedure according TS 36.508 [94] subclause 4.5A.15, applied to the identity of the Default EPS Bearer of the emergency PDN.

Specific Message Contents

INVITE (step 1 of Annex C.22)

Use the default message “INVITE for MO call setup” in annex A.2.1. with the following conditions:

- A7 “INVITE for creating an emergency session within an emergency registration” shall apply; and
- A8 “UE is capable of obtaining location information, has obtained its location and is setting up an emergency session “ shall apply.

180 Ringing for INVITE (step 3 of Annex C.22)

Use the default message “180 Ringing for INVITE” in annex A.2.6 The condition A4 “180 sent by the SS when setting up an emergency call” shall apply.

200 OK for INVITE (step 4 of Annex C.22)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1. The condition A6 “Response sent by SS for INVITE for emergency call” shall apply

BYE (Step 16)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 17)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

19.1.1.5 Test requirements

If the UE is capable of obtaining location information the INVITE request sent for initiating the emergency call shall contain a Geolocation header. The body of an INVITE request containing the Geolocation header must contain a PIDF location object. The PIDF-LO shall be syntactically correct (as specified within RFC 4119 [99]) and it shall be mapped to the same Content-ID which can be found from the Geolocation header.

19.1.2 Emergency call with emergency registration / Success / Location information not available

19.1.2.1 Definition

Test to verify that the UE can correctly register to IMS emergency services and initiate an IMS emergency call when UE is registered to IMS non-emergency services of the HPLMN either with ISIM or USIM. The process consists of setting up EPS emergency bearers, sending initial emergency registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally initiating the emergency call. In this case the location information is not available to the UE.

19.1.2.2 Conformance requirement

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

...

8) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

…

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.6.8.3 (release 9)

19.1.2.3 Test purpose

1) To verify that if the location information is not available UE will not add Geolocation header or PIDF-LO to the INVITE request for emergency call, as defined within 3GPP TS 24.229 [10] clause 5.1.6.8.3.

19.1.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test environment shall ensure that UE can not access any information (such as GPS signal) from which the UE would be able to derive its geographical location. The UE shall only be able to read the global cell ID as provided by the SS.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call.

16) Call is released on the UE using Annex C.32 procedure

17) Void

18) Emergency Bearer context is deactivated

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
16-16A4	→		Steps defined in Annex C.32	The UE releases the call
17			Void	
18			EPS emergency bearer context deactivation by the SS.	EPS Bearer Deactivation procedure according TS 36.508 [94] subclause 4.5A.15, applied to the identity of the Default EPS Bearer of the emergency PDN.

Specific Message Contents

INVITE (Step 1 of Annex C.22)

Use the default message “INVITE for MO call setup” in annex A.2.1. The condition A7 “INVITE for creating an emergency session within an emergency registration” shall apply. In this test case condition A8 shall not apply as the UE is not able to obtain its geographical location.

180 Ringing for INVITE (Step 3 of Annex C.22)

Use the default message “180 Ringing for INVITE” in annex A.2.6 The condition A4 “180 sent by the SS when setting up an emergency call” shall apply.

200 OK for INVITE (Step 4 of Annex C.22)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1. The condition A6 “Response sent by SS for INVITE for emergency call” shall apply

BYE (Step 16)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 17)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

19.1.2.5 Test requirements

The INVITE request sent for initiating the emergency call shall not contain a Geolocation header and the body of the request must not contain a PIDF location object.

19.1.3 Emergency call with emergency registration / Abnormal case / IM CN sends a 380 / UE performs emergency call via CS domain / UTRAN or GERAN

19.1.3.1 Definition

Test to verify that the UE performs a emergency call via CS domain, when attempt to initiate an IMS emergency call is rejected by 380 for a UE registered to IMS emergency services and IMS non-emergency services of the HPLMN either with ISIM or USIM. The process consists of setting up EPS emergency bearers, sending initial emergency registration to S-CSCF via the P-CSCF discovered, authenticating the user , initiating the emergency call. The emergency call is rejected with 380 and UE performs emergency call via supported CS domain over UTRAN or GERAN.

19.1.3.2 Conformance requirement

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 and 3GPP TS 23.167 to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

...

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

- the first entry in the list of public user identities provisioned in the UE;

- the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and

- the derived temporary public user identity, in all other cases.

[TS 24.229 clause 5.1.6.8.1]:

The UE shall translate any user indicated emergency number as specified in 3GPP TS 22.101 to an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031.

…

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response including a 3GPP IM CN subsystem XML body as described in subclause 7.6 that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall automatically send an ACK request to the P-CSCF as per normal SIP procedures and terminate the session. In addition, if the 380 (Alternative Service) response includes a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration:

- the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element; and

- one of subclause 5.1.6.8.3 or subclause 5.1.6.8.4 applies.

NOTE 2: Emergency numbers which the UE does not detect, will be treated as a normal call.

NOTE 3: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442; or

- if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119, include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442;

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

In the event the UE receives a 380 (Alternative Service) response with a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration, and the Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the following treatment is applied:

1) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), then the UE shall:

   a) if the CS domain is available to the UE, and no prior attempt using the CS domain for the current emergency call attempt has been made, attempt emergency call via CS domain using appropriate access technology specific procedures; and

   b) if the CS domain is not available to the UE or the emergency call has already been attempted using the CS domain, then perform one of the following actions:

      - if the <action> child element of the <alternative-service> child element of the <ims-3gpp> element in the IM CN subsystem XML body as described in subclause 7.6 is set to "emergency-registration" (see table 7.7AB), perform an initial emergency registration using a different VPLMN if available, as described in subclause 5.1.6.2 and if the new emergency registration succeeded, attempt an emergency call as described in this subclause; or

      - perform implementation specific actions to establish the emergency call; and

2) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA) then the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 5: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

[TS 24.229 annex L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

...

When activating a EPS bearer context to perform emergency registration, the UE shall request a PDN connection for emergency bearer services as described in 3GPP TS 24.301. The procedures for EPS bearer context activation and P-CSCF discovery, as described in subclause L.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 will be considered as a visited network.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.1, 5.1.6.8.3, and Annex L2.2.6 (release 9)

19.1.3.3 Test purpose

1) To verify that the on reception of 380 Alternate Service for an INVITE sent for emergency call establishment, UE initiates the emergency call in supported CS domain over UTRAN or GERAN.

19.1.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN , GERAN cell 24
- Cell A power level is set as “serving cell” and cell 24/cell 5 power level is set as “suitable cell”

Note: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) IMS emergency call is initiated on the UE.

2)-5) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 2 to 15 and parallel behaviour steps 1-4 for EPS emergency bearer context activation, and subsequent IMS emergency registration,

6) UE sends INVITE for emergency call.

7) SS responds with 380 Alternative services.

8) UE ACKS the 380 Alternative service message. UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM/GMM registration if necessary.

9) CS emergency call is established and released. For GERAN cell, UE performs MM/GMM registration after CS call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-5			Steps defined in annex C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
6	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports
7	<-		380 Alternative Service	The SS responds with a 380 Alternative Service response
8	→		ACK	The UE acknowledges the receipt of 380 Alternative Service for INVITE NOTE 1: Step 8 can happen in parallel to step 8Aa1.
-	-		EXCEPTION: Within 2 seconds of step 7 the UE may transmit EXTENDED SERVICE REQUEST OR PDN_DISCONNECT_REQUEST (or both). DEACTIVATE EPS BEARER CONTEXT REQUEST is sent if EXTENDED SERVICE REQUEST is not received within one second after PDN DISCONNECT REQUEST. Steps 8AAa1 to Step 8AAa4 OR 8AAb1 to 8AAb3 OR 8AAc1 to 8AAc2 OR 8AAd1 can happen	NOTE 2: Value of 2 seconds is based on estimation.
8AAa1	->		PDN DISCONNECT REQUEST	UE sends PDN disconnect request during CS fallback procedure triggered
8AAa2	<-		DEACTIVATE EPS BEARER CONTEXT REQUEST	SS responds with DEACTIVATE EPS BEARER CONTEXT REQUEST after 1s
8AAa3	->		DEACTIVATE EPS BEARER CONTEXT ACCEPT	UE sends DEACTIVATE EPS BEARER CONTEXT ACCEPT
8AAa4	->		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27
8AAb1	->		PDN DISCONNECT REQUEST	UE sends PDN disconnect request during CS fallback procedure triggered
8AAb2	<-		DEACTIVATE EPS BEARER CONTEXT REQUEST	SS responds with DEACTIVATE EPS BEARER CONTEXT REQUEST after 1s
8AAb3	->		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27
8AAc1	->		PDN DISCONNECT REQUEST	UE sends PDN disconnect request during CS fallback procedure triggered
8AAc2	->		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27 within 1s of step 8AAc1
8AAd1	->		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27
8Aa0a1 - 8Aa0a3			Void	
8Aa1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends Extended service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8Aa2	<-		SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
-	-		EXCEPTION: Either step 9a1 or 9b1 is performed, depending on the value of px_RATComb_Tested	

9a1	-	IF px_RATComb_Tested = EUTRA_UTRA UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN) and performs emergency call in CS domain together with MM/GMM registration	NOTE3: RAU procedure can take place in parallel to emergency CS call. If the Service category IE is included, then SS verifies that the Emergency Service Category IE bit 6 and bit 7 are set to 0
-	-	EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration/deregistration defined in Annex C.46/C.30 of TS 34.229-1 can take place	-
9a2	-	SS configures cell A as a “non-suitable cell”	-
9a3	-	Emergency CS call is released	-
9b1	-	IF px_RATComb_Tested = EUTRA_GERAN UE performs CS fallback or cell reselection to a cell supporting CS domain (GERAN cell) and performs emergency call in CS domain	If the Service category IE is included, then SS verifies that the Emergency Service Category IE bit 6 and bit 7 are set to 0
9b2	-	SS configures cell A as a “non-suitable cell”	-
9b3	-	Emergency CS call is released	-
9b4	-	UE performs MM/GMM registration	-

Specific Message Contents

INVITE (Step 6)

Use the default message “INVITE for MO call setup” in annex A.2.1. with the following conditions:

- A7 “INVITE for creating an emergency session within an emergency registration” shall apply;

ACK (Step 8)

Use the default message “ACK” in Annex A.2.7.

380 Alternative Service (Step 7)

Use the default message “380 Alternative Service” in annex A.4.1.

RRCConnectionRelease (step 8Aa2)

Use the default message with the following specific contents

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
Geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (step 9b4)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

19.1.3.5 Test requirements

In step 9a1 or 9b1, UE initiates a CS emergency call in UTRAN or GERAN cell (respectively). When the service category IE is included, UE shall send the Emergency Service Category IE bit 6 and bit 7 set to 0.

19.1.3a Emergency call with emergency registration / Abnormal case / IM CN sends a 380 / UE performs emergency call via CS domain / CDMA 2000 1xRTT

19.1.3a.1 Definition

Same as in 19.1.3.1, except: UE performs emergency call via supported CS domain over CDMA 2000 1xRTT.

19.1.3a.2 Conformance requirement

Same Conformance requirement as in clause 19.1.3.2

19.1.3a.3 Test purpose

1) To verify that the on reception of 380 Alternate Service for an INVITE sent for emergency call establishment, UE initiates the emergency call in supported CS domain CDMA 2000 1xRTT

19.1.3a.4 Method of test

Initial conditions

Same as in 19.1.3.4, except: UE contains ISIM and USIM and CSIM or USIM and CSIM applications on UICC.

The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell A
- 1xRTT cell 19
- Cell A power level is set as “serving cell” and cell 19 power level is set as “suitable cell”

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

Same as in 19.1.3.4

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-5			Steps defined in annex C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
6	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports
7	<-		380 Alternative Service	The SS responds with a 380 Alternative Service response
8	→		ACK	The UE acknowledges the receipt of 380 Alternative Service for INVITE
9			UE performs cell reselection to a cell supporting CS domain (CDMA2000 1XRTT cell) and performs emergency call in CS domain after CDMA registration (if needed)	
10			CS call is released	

Specific Message Contents

Same as in 19.1.3.4

19.1.3a.5 Test requirements

In step 9, UE initiates a CS emergency call in 1xRTT cell.

19.1.3b Void

19.1.3c Emergency call with emergency registration / Abnormal case / IM CN sends 503 Service Unavailable / UE performs emergency call via CS domain / UTRAN or GERAN

19.1.3c.1 Definition

Test to verify that the UE performs an emergency call via CS domain, when attempt to initiate an IMS emergency call is rejected by 503 for a UE registered to IMS emergency services and IMS non-emergency services either with ISIM or USIM.

19.1.3c.2 Conformance requirement

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 and 3GPP TS 23.167 to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

[TS 24.229 annex L.2.2.6]:

Upon receiving a 3xx other than 380 (Alternative service), 4xx, 5xx or 6xx response to an INVITE request for a UE detectable emergency call, the UE shall perform domain selection as specified in 3GPP TS 23.167 [4B] annex H, to re-attempt the emergency call.

[TS 23.167 annex H.5]:

This clause details the domain priority and selection (see clause 7.3) for UE that attempts to make an emergency session for UTRAN, E-UTRAN or NG-RAN radio access networks based on the UE attach status to CS or PS domains and the network support for IMS emergency and IMS voice over PS.

The following table (Table H.1) defines these rules based on the UE (last 2 columns) for different initial conditions (first 4 columns) when an emergency session is initiated and when the UE is not in limited service state.

For NG-eCall (eCall over IMS) domain selection in clause H.6 applies. This clause is not applicable for NG-eCall.

Table H.1: Domain Selection Rules for emergency session attempts for UTRAN, E-UTRAN or NG-RAN radio access networks

	CS Attached	PS Attached	VoIMS	EMS	First EMC Attempt	Second EMC Attempt
A	N	Y	Y	Y	PS	CS if available and supported - NOTE 7)
B	N	Y	N	Y	PS or CS if the emergency session includes at least voice. PS if the emergency session contains only media other than voice.	PS if first attempt in CS CS if first attempt in PS - NOTE 7)
C	N	Y	Y or N	N	PS if ESFB is "Y" (NOTE 5). Else CS or PS for another 3GPP RAT with EMS or ESFB set to "Y" if available and supported and if the emergency session includes at least voice. Else PS for another 3GPP RAT with EMS or ESFB set to "Y" if available and supported if the emergency session contains only media other than voice.	PS if first attempt in CS CS if first attempt in PS - NOTE 7)
D	Y	N	Y or N	Y or N	CS if the emergency session includes at least voice. PS if available and EMS or ESFB is "Y" and emergency session contains only media other than voice.	PS if available and EMS or ESFB is "Y"
E	Y	Y	Y	Y	If the emergency session includes at least voice, follow rules in TS 22.101 [8] which say to use the same domain as for a non-EMC (NOTE 2) PS if the emergency session contains only media other than voice.	PS if first attempt in CS CS if first attempt in PS
F	Y	Y	Y or N	N	PS if ESFB is "Y" (NOTE 5). Else PS for another 3GPP RAT with EMS if available and supported or CS, if the emergency session includes at least voice.	CS if first attempt in PS PS for another 3GPP RAT if available and supported and EMS or ESFB is "Y" if first attempt in CS.

G	Y	Y	N	Y	CS if the emergency session includes at least voice. PS if the emergency session contains only media other than voice.	PS

EMC = Emergency Session. EMC includes also normal calls initiated in the CS domain that are treated by the CS CN as emergency calls.
VoIMS = Voice over IMS over PS sessions support as indicated by IMS Voice over PS session supported indication as defined in TS 23.401 [28], TS 23.060 [2] and TS 23.502 [49].
EMS = IMS Emergency Services supported as indicated by Emergency Service Support indicator as defined in TS 23.401 [28], TS 23.060 [2], TS 23.501 [48] and TS 23.502 [49].
ESFB = Emergency Services Fallback for 5GS as defined in TS 23.501 [48] and TS 23.502 [49].
NOTE 1: If the UE selects the CS domain and initiates a normal call using the dialled local emergency number (see clause 7.1.2), and the UE enters limited service state (e.g. due to a Location Registration failing), then the UE camps on an acceptable cell (see TS 23.122 [41]) and may proceed with the EMC by initiating an emergency call in limited service state.
NOTE 2: Use of the same domain as for a non-EMC is restricted to UTRAN, E-UTRAN and NG-RAN access (e.g. excludes WLAN).
NOTE 3: This NOTE applies to a UE in dual registration mode as defined in TS 23.501 [48]. A dual registration mode UE that is registered to both EPC and 5GC assumes attachment, for the purpose of the "PS Attached" column, to whichever of EPC or 5GC indicates EMS as "Y". When both EPC and 5GC indicate EMS as "Y", the UE shall assume attachment to either EPC or 5GC based on implementation. A UE that is registered to both EPC and 5GC does not use emergency services fallback and ignores the ESFB condition when performing domain selection.
NOTE 4: The other 3GPP RAT for row C and row F can be any of UTRA, E-UTRAN connected to EPC, E-UTRA connected to 5GC or NR connected to 5GC that is supported by the UE and differs from the RAT to which the UE is currently attached in the PS domain (or is assumed to be attached based on NOTE 3).
NOTE 5: The condition 'ESFB is "Y"' only applies for a UE that is camped on or connected to 5GS via NR or via E-UTRA and that supports Emergency Services Fallback. In that case the emergency call will be provided over E-UTRAN or E-UTRA connected to 5GC as defined in procedures in TS 23.502 [49]. The condition 'ESFB is "Y"' is taken into consideration by the UE only when the network has indicated EMS = "N" for the RAT on which the UE is camping or connected.
NOTE 6: For 5GS, the value of the column "EMS" is for the RAT that UE is camped on or is connected to.
NOTE 7: As an implementation option, when the first attempt uses PS and fails for reasons other than related to IMS, the second attempt may use PS with a different 3GPP RAT. In this case the UE, can make a third attempt using CS.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.1 and Annex L.2.2.6, and TS 23.167 [141], annex H.5.

19.1.3c.3 Test purpose

1) To verify that on reception of 503 Service Unavailable for an INVITE sent for emergency call establishment, UE initiates the emergency call in supported CS domain over UTRAN or GERAN.

19.1.3c.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN , GERAN cell 24
- Cell A power level is set as “serving cell” and cell 24/cell 5 power level is set as “suitable cell”

Note: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) IMS emergency call is initiated on the UE.

2)-5) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 2 to 15 and parallel behaviour steps 1-4 for EPS emergency bearer context activation, and subsequent IMS emergency registration,

6) UE sends INVITE for emergency call.

7) SS responds with 503 Service Unavailable.

8) UE ACKS the Service Unavailable message. UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM/GMM registration if necessary.

9) CS emergency call is established and released. For GERAN cell, UE performs MM/GMM registration after CS call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-5			Steps defined in annex C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
6	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports
7	<-		503 Service Unavailable	The SS responds with 503 Service Unavailable response
8	→		ACK	The UE acknowledges the receipt of 503 Service Unavailable for INVITE NOTE 1: Step 8 can happen in parallel to step 8Aa1.
-	-		EXCEPTION: Within 2 seconds of step 7 the UE may transmit EXTENDED SERVICE REQUEST OR PDN_DISCONNECT_REQUEST (or both). DEACTIVATE EPS BEARER CONTEXT REQUEST is sent if EXTENDED SERVICE REQUEST is not received within one second after PDN DISCONNECT REQUEST. Steps 8AAa1 to Step 8AAa4 OR 8AAb1 to 8AAb3 OR 8AAc1 to 8AAc2 OR 8AAd1 can happen	NOTE 2: Value of 2 seconds is based on estimation.
8AAa1	->		PDN DISCONNECT REQUEST	UE sends PDN disconnect request during CS fallback procedure triggered
8AAa2	<-		DEACTIVATE EPS BEARER CONTEXT REQUEST	SS responds with DEACTIVATE EPS BEARER CONTEXT REQUEST after 1s
8AAa3	->		DEACTIVATE EPS BEARER CONTEXT ACCEPT	UE sends DEACTIVATE EPS BEARER CONTEXT ACCEPT
8AAa4	->		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27
8AAb1	->		PDN DISCONNECT REQUEST	UE sends PDN disconnect request during CS fallback procedure triggered
8AAb2	<-		DEACTIVATE EPS BEARER CONTEXT REQUEST	SS responds with DEACTIVATE EPS BEARER CONTEXT REQUEST after 1s
8AAb3	->		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27
8AAc1	->		PDN DISCONNECT REQUEST	UE sends PDN disconnect request during CS fallback procedure triggered
8AAc2	->		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27 within 1s of step 8AAc1
8AAd1	->		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27
8Aa1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends Extended service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8Aa2	<-		SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
-	-		EXCEPTION: Either step 9a1-9a3 or 9b1-9b3 are performed, depending on the value of px_RATComb_Tested	

9a1	-	IF px_RATComb_Tested = EUTRA_UTRA UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN) and performs emergency call in CS domain together with MM/GMM registration	NOTE3: RAU procedure can take place in parallel to emergency CS call. If the Service category IE is included, then SS verifies that the Emergency Service Category IE bit 6 and bit 7 are set to 0
-	-	EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration defined in Annex C.46 of TS 34.229-1 can take place	-
9a2	-	SS configures cell A as a “non-suitable cell”	-
9a3	-	Emergency CS call is released	-
9b1	-	IF px_RATComb_Tested = EUTRA_GERAN UE performs CS fallback or cell reselection to a cell supporting CS domain (GERAN cell) and performs emergency call in CS domain	If the Service category IE is included, then SS verifies that the Emergency Service Category IE bit 6 and bit 7 are set to 0
9b2	-	SS configures cell A as a “non-suitable cell”	-
9b3	-	Emergency CS call is released	-
9b4	-	UE performs MM/GMM registration	-

Specific Message Contents

INVITE (Step 6)

Use the default message “INVITE for MO call setup” in annex A.2.1. with the following conditions:

- A7 “INVITE for creating an emergency session within an emergency registration” shall apply;

ACK (Step 8)

Use the default message “ACK” in Annex A.2.7.

503 Service Unavailable (Step 7)

Use the default message “503 Service Unavailable” in annex A.4.2.

RRCConnectionRelease (step 8Aa2)

Use the default message with the following specific contents

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
Geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (step 9b4)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

19.1.4 Void

19.1.5 Emergency call with emergency registration / Emergency SIP signalling and media in parallel with another ongoing IM CN subsystem signalling and media

19.1.5.1 Definition

Test to verify that the UE [IMS registered for non-emergency services and ongoing multimedia call] can correctly register to IMS emergency services and initiate an IMS emergency call when UE is registered to IMS non-emergency services of the HPLMN either with ISIM or USIM. The process consists of setting up EPS emergency bearers, sending initial emergency registration to E-CSCF via the P-CSCF discovered, authenticating the user and finally initiating the emergency call.

19.1.5.2 Conformance requirement

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 and 3GPP TS 23.167 to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

...

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 [4B] and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sop" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

- the first entry in the list of public user identities provisioned in the UE;
- the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and
- the derived temporary public user identity, in all other cases.

When the UE performs an initial emergency registration and whilst this emergency registration is active, the UE shall:

- handle the emergency registration independently from any other ongoing registration to the IM CN subsystem;
- handle any signalling or media related IP-CAN for the purpose of emergency calls independently from any other established IP-CAN for IM CN subsystem related signalling or media; and
- handle all SIP signalling and all media related to the emergency call independently from any other ongoing IM CN subsystem signalling and media.

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tell URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a Request-URI in the INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sops" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

3) the UE shall insert in the INVITE request, a To header field with:

   - the same emergency service URN as in the Request-URI; or
   - if the UE cannot perform local dial string interpretation for the dialled digits, a dial string URI representing the dialled digits in accordance with RFC 4967 [103] or a tell URL representing the dialled digits;

NOTE 1: This version of this document does not provide any specified handling of a URI with the dialled digits in accordance with RFC 4967 [103] at an entity within the IM CN subsystem. Behaviour when this is used is therefore not defined.

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tell URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 3: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, then the UE shall include its location information in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Relocation header field, set the Relocation-Routing header field to "yes", all in accordance with RFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, and set the Geolocation-Routing header field to "yes", all in accordance with RFC 6442 [98]; and

NOTE 4: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

8) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 5: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

   - if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

<discussion see above>

[TS 24.229 annex L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

...

When activating a EPS bearer context to perform emergency registration, the UE shall request a PDN connection for emergency bearer services as described in 3GPP TS 24.301. The procedures for EPS bearer context activation and P-CSCF discovery, as described in subclause L.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 will be considered as a visited network.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.3 and Annex L2.2.6 (release 9)

19.1.5.3 Test purpose

1) To verify that the UE registered for non-emergency services and ongoing multimedia call, on initiation of an emergency call, holds the ongoing multimedia call and sends a correctly composed INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.3 and 6.1.2.

19.1.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step and thereafter executing the generic test procedure in Annex C.21 up to its last step for a multimedia non-emergency call.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Ongoing multimedia call is put on hold.

2) IMS emergency call is initiated on the UE.

3)-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call establishment with PSAP.

15A User initiates resumption of Multimedia call.

16-17) UE releases the emergency call.

18) Void.

19-24) Multimedia call is resumed and released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates hold of ongoing call	
2-5	→		Steps defined in annex C.8	Ongoing call is put on hold by UE
6			User initiates an emergency call	
7-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
15A			User resumes the ongoing call which is on hold	Triggers release of the emergency call.
16-17			The UE releases the emergency call using steps 2-5 of Annex C.32	
18			Void	
19-22			Steps defined in Annex C.8	Ongoing call is resumed.
23	→		BYE	The UE releases the multimedia call
24	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

INVITE (step 1 in procedure in Annex C.22)

Use the default message “INVITE for MO call setup” in annex A.2.1. with the following conditions:

- A7 “INVITE for creating an emergency session within an emergency registration” shall apply;

19.1.5.5 Test requirements

In steps 7-15, UE performs emergency registration and establishes an emergency call

19.1.6 Emergency call with emergency registration / Success / GIBA against a network with GIBA support only

19.1.6.1 Definition

Test to verify that the UE can correctly register to IMS emergency services in a visited network with support for GIBA only, while the home network used for IMS registration supports IMS security, when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial emergency registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally sending an emergency session initiation.

19.1.6.2 Conformance requirement

[TS 24.229 Rel-8, clause 5.1.1.2.1]

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4).

[TS 24.229 Rel-9, clause 5.1.1.2.1]

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 4: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

[TS 24.229 Rel-9, clause 5.1.1.2.6]

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support for GPRS-IMS-Bundled authentication.

b) the Security-Client header field as defined in RFC 3329 shall not be included;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

[TS 24.229 Rel-9, clause 5.1.1.5.3]

On receiving a 420 (Bad Extension) in which the Unsupported header field contains the value "sec-agree" and if the UE supports GPRS-IMS-Bundled authentication, the UE shall initiate a new authentication attempt with the GPRS-IMS-Bundled authentication procedures as specified in subclause 5.1.1.2.6.

[TS 24.229 Rel-9, clause 5.1.2A.1.1]

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using either a given contact address or to the registration flow and the associated contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

…

- if GPRS-IMS-Bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2.

…

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

   - if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627; or

   - if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627; or

- otherwise, a SIP URI containing the contact address of the UE;

NOTE 7: The above items are mutually exclusive.

2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626;

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841, the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and

4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841, the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

…

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

Reference(s)

TS 24.229 [10] clauses 5.1.1.2.1, 5.1.1.2.6, 5.1.1.5.3 and 5.1.2A.1.1.

19.1.6.3 Test purpose

1) To verify that after receiving a 420 (Bad Extension) response the UE sends a correctly composed initial REGISTER request for IMS emergency services.

2) To verify that after receiving a 200 OK response for the REGISTER without security-client header, the UE successfully initiates an IMS emergency call.

19.1.6.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the NW is VPLMN and the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1)-12) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 12 and parallel behaviour steps 1 for EPS emergency bearer context activation,

13) SS waits for the UE to send an initial REGISTER request containing “sos” SIP URI parameter in the Contact header field.

14) The SS responds to the REGISTER request with a 420 Bad Extension response,

15) The UE initiates IMS registration indicating support of GIBA. SS waits for the UE to send an initial REGISTER request.

16) The SS responds to the REGISTER request with valid 200 OK response,

17) The SS waits for the UE to send an INVITE request.

18)-20A) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 13 to 15 and parallel behaviour Steps 2-5 defined in annex C.22 of TS 34.229-1 for IMS Emergency call for EPS is established,

21)-24A) The UE releases the call.

25)-26) The SS deactivates EPS emergency bearer context.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-12			Steps defined in TS 36.508 [94] table 4.5A.4.3-1	EPS Bearer Activation procedure and IP address allocation according TS 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
13	→		REGISTER	UE sends initial registration for IMS services.
14	←		420 Bad Extension	The SS responds with a failure.
15	→		REGISTER	The UE sends initial registration for IMS services indicating support for GIBA procedure by not including an Authorization header field.
16	←		200 OK	The SS responds with 200 OK.
17	→		INVITE	UE sends INVITE request.
18-20A			Steps 2 to 5 defined in annex C.22	IMS emergency call setup with PSAP
21-24A	→		Steps defined in annex C.32	The UE releases the call
25-26			EPS emergency bearer context deactivation by the SS.	EPS Bearer Deactivation procedure according TS 36.508 [94] subclause 4.5A.15, applied to the identity of the Default EPS Bearer of the emergency PDN.

Specific Message Contents

REGISTER (Step 13)

Use the default message “REGISTER” in annex A.1.1 with condition A1 "Initial unprotected REGISTER" and A7 “Initial unprotected or subsequent REGISTER for emergency registration”

420 Bad Extension for REGISTER (Step 14)

Use the default message “420 Bad Extension for REGISTER” in annex A.1.8 with condition A1 “IMS emergency registration failure for an anonymous emergency call”.

REGISTER (Step 15)

Use the default message “REGISTER” in annex A.1.1 with condition A7 “Initial unprotected or subsequent REGISTER for emergency registration”.

200 OK for REGISTER (Step 16)

Use the default message “200 OK for REGISTER” in annex A.1.3 with condition A2 “GIBA”

INVITE (Step 17)

Use the default message “INVITE” in annex A.2.1 with condition A19 “INVITE for creating an emergency session within an emergency registration using GIBA”.

19.1.6.5 Test requirements

The UE shall send requests and responses as described in clause 19.1.6.4.

19.2 Void

19.3 Non-UE detectable emergency call

19.3.1 Non-UE detectable emergency call / IM CN sends a 1xx response / UE geographical location information available or not

19.3.1.1 Definition

Test to verify that the UE acts correctly when it receives a 1xx response to an initial request for a dialog from the IM CN, the response containing a P-Asserted-Identity header field set to an emergency number that is recognisable by the UE and the UE sends an UPDATE request with:

- Geolocation header and information if the UE is capable of obtaining location information; and
- Contact header set appropriately

19.3.1.2 Conformance requirement

If the UE receives a 1xx or 200 (OK) response to an initial request for a dialog, the response containing a P-Asserted-Identity header field set to an emergency number as specified in 3GPP TS 22.101, and:

- if a public GRUU value (pub-gruu) has been saved associated with the public user identity, the public GRUU value has not been included in the Contact header field of the initial request for a dialog as specified in RFC 5627;
- if a public GRUU value (pub-gruu) has not been saved and a protected server port was not included in the address in the Contact header field of the initial request for a dialog; or
- if the UE has its geographical location information available and the geographical location information has not been included in the initial request for a dialog;

then the UE shall send an UPDATE request according to RFC 3311; and

1) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the UE shall include in the UPDATE request a P-Access-Network-Info header field and it shall contain a location identifier such as the cell id or the identity of the I-WLAN access node;
2) if the UE has its geographical location information available, then the UE shall include it in the UPDATE request in the following way:
   I) if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field and set the "inserted-by" parameter to indicate its hostport, all in accordance with RFC 6442 and set the "inserted-by" parameter to indicate its hostport, all in accordance with draft-ietf-sipcore-loca; or
   II) if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442. The Geolocation header field is set to a Content ID and set the "inserted-by" parameter to indicate its hostport, all in accordance with RFC 6442;
3) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442; and
4) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity, then the UE shall insert the public GRUU ("pub-gruu" header field parameter) value in the Contact header field of the UPDATE request as specified in RFC 5627; otherwise the UE shall include the address in the Contact header field set in accordance with subclause 5.1.6.8.4, item 8.

NOTE 1: The IMS emergency specification in 3GPP TS 23.167 describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.10

19.3.1.3 Test purpose

To verify that if the UE is not able to detect that an emergency number has been dialled:

- in the event the UE receives a 1xx response to an INVITE request the response containing a P-Asserted-Identity header field set to an emergency number, the UE:
  - If the UE is able to obtain its geolocation and the geographical location information has not been included in the initial request for a dialog; then the UE shall include its geolocation information in the UPDATE message
  - If the UE is not able to obtain its geolocation the UE does not include it in the UPDATE message
  - includes a Contact header in the UPDATE message with the correct contents

19.3.1.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC.

Test environment shall be set up to provide the needed input to the UE, in order for the UE to derive its location, if the UE is capable of obtaining location information. This shall be done by use of the test function Update UE Location Information defined in TS 34.109 [117] or in TS 36.509 [118] depending on the RAT being used in the test case, if supported by the UE according to pc_UpdateUE_LocationInformation. Otherwise, or in addition any other suitable method may also be used.

UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

1) A non-emergency MO call is initiated up following the generic procedure in Annex C.21.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-13				Steps 1-13 of Annex C.21. The UE initiates a non-emergency call.

Specific Message Contents INVITE (Step 2)

Use the default message "INVITE" in annex A.2.1 without options A6, A7 and A8.

183 Session in Progress (Step 4)

Use the default message "183 Session in Progress" in annex A.2.3 with option A5.

UPDATE (Step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Cond	Value/remark	Rel	Reference
Geolocation	A1		Rel-9	RFC 6442 [98]
locationURI		cid-url indicating the Content-Id of the PIDF-LO within the multipart MIME body of INVITE request. (Note that location-by-reference URI is not allowed as the SS does not provide any external storage for location info for the UE to refer.)		
Geolocation-Routing	A1	"yes"	Rel-9	RFC 6442
Contact				RFC 3261 [15] RFC 5627 [61]
addr-spec	A2	Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response		
addr-spec	A3	SIP URI with IP address or FQDN and protected server port of UE		
addr-spec	A4	SIP URI with IP address or FQDN and unprotected server port of UE		
Content-Type				
media-type	A1 not A1	*multipart/mixed* *application/sdp*		TS 24.229 [10] RFC 3261 [15]
Message-body		If condition A1 applies, the multipart-mime body shall also contain a PIDF-LO element mapped to the same Content-ID which can be found from the Geolocation header The PIDF-LO shall contain at least the following elements: - One or more 'geopriv' elements, each containing: - One 'location-info' element describing the location of the UE; and - One 'usage-rules' element describing the limitations of the usage of the location info.		RFC 6442 [98]

Condition	Explanation
A1	UE is capable of obtaining location information
A2	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A3	Not A2 and (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A4	Not A2 and (GIBA, A.6a/1 3GPP TS 34.229-2 [5])

180 Ringing (Step 9)

Use the default message "180 Ringing" in annex A.2.6 with options A4 and A8.

200 OK (Step 12)

Use the default message "200 OK" in annex A.3.1 with option A6.

19.3.1.5 Test requirements

SS must check that in:

- Step 2 the UE sends a non-emergency INVITE with the correct contents
- Step 7 the UE sends the UPDATE message with:
    - the Geolocation header set appropriately, if the UE is capable of obtaining location information
    - Contact header set appropriately

19.3.2 Non-UE detectable emergency call / IM CN sends 380 Alternative Service including emergency service URN and no emergency subservice type / Non-emergency IMS registration / UTRAN or GERAN

19.3.2.1 Definition

Test to verify that the UE correctly requests an emergency service on CS domain over UTRAN or GERAN if the UE has received a 380 (Alternative Service) response to an INVITE request with Contact header field in which an emergency service information is included with no emergency subservice type.

19.3.2.2 Conformance requirement

[TS 24.229 Rel-9, clause L.2.2.6]

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

Some jurisdictions allow emergency calls to be made when the UE does not contain an ISIM or USIM, or where the credentials are not accepted. Additionally where the UE is in state EMM-REGISTERED.LIMITED-SERVICE and EMM-REGISTERED.PLMN-SEARCH, a normal ATTACH has been attempted and it can also be assumed that a registration in the IM CN subsystem will also fail. In such cases, the procedures for emergency calls without registration apply, as defined in subclause 5.1.6.8.2.

When activating a EPS bearer context to perform emergency registration, the UE shall request a PDN connection for emergency bearer services as described in 3GPP TS 24.301 [8J]. The procedures for EPS bearer context activation and P-CSCF discovery, as described in subclause L.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE 1: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] will be considered as a visited network.

The type of emergency service for an emergency number is derived from the settings of the emergency service category value (bits 1 to 5 of the emergency service category value as specified in subclause 10.5.4.33 of 3GPP TS 24.008 [8]). Table L.2.2.6.1 below specifies mappings between a type of emergency service and an emergency service URN. The UE shall use the mapping to match an emergency service URN and a type of emergency service. If a dialled number is an emergency number but does not map to a type of emergency service the service URN shall be "urn:service:sos".

Table L.2.2.6.1: Mapping between type of emergency service and emergency service URN

Type of emergency service	Emergency service URN
Police	urn:service:sos.police
Ambulance	urn:service:sos.ambulance
Fire Brigade	urn:service:sos.fire
Marine Guard	urn:service:sos.marine
Mountain Rescue	urn:service:sos.mountain

If the IP-CAN did not provide a local emergency number that matches the dialled number (see subclause 5.1.6.1) and multiple types of emergency service can be derived for a dialled number from the information configured on the USIM then:

- if the UE is in the HPLMN, the UE shall map any one of these types of emergency service to an emergency service URN as specified in table L.2.2.6.1; and

- if the UE is in the VPLMN, the UE shall select "urn:service:sos".

If the IP-CAN provided a local emergency number that matches the dialled number (see subclause 5.1.6.1), and:

- if the UE can derive one or more types of emergency service from the information received from the IP-CAN for the dialled number and the UE cannot derive types of emergency service from the information configured on the USIM for the dialled number; or

- if the UE is able to derive identical types of emergency service from both the information received from the IP-CAN for the dialled number and from the information configured on the USIM for the dialled number,

then the UE shall map any one of these emergency service types to an emergency service URN as specified in table L.2.2.6.1.

NOTE 2: How the UE resolves clashes where an emergency number is associated with one or more different types of emergency service configured in the USIM and in information received from the access network, is implementation dependent.

Upon reception of a 380 (Alternative Service) response to an INVITE request as defined in subclause 5.1.3.1, if:

- the 380 (Alternate Service) response contains a Contact header field;

- the value of the Contact header field is a service URN; and

- the service URN has a top-level service type of "sos";

then the UE determines that "emergency service information is included" as described 3GPP TS 23.167 [4B], else the UE determines that "emergency service information" as described 3GPP TS 23.167 [4B] is not included.

If the "emergency service information is included" as described 3GPP TS 23.167 [4B]:

1) if the URN in the Contact header field matches an emergency service URN in table L.2.2.6.1, then the type of emergency service is the value corresponding to the matching entry in table L.2.2.6.1; and

2) if the URN in the Contact header field does not match any emergency service URN in table L.2.2.6.1, then the type of emergency service is not identified.

NOTE 3: In bullet 2), the URN in the Contact header field either contains "no emergency subservice type" as described in 3GPP TS 23.167 [4B] triggering an emergency call, or contains an "emergency subservice type that does not map into an emergency service category for the CS domain" as described in 3GPP TS 23.167 [4B] triggering a normal call when the dialled number is available or triggering an emergency call when the dialled number is not available.

Reference(s)

3GPP TS 24.229 [10], clause L.2.2.6

19.3.2.3 Test purpose

To verify that on reception of 380 Alternative Service with a Contact header field with value "urn:service:sos" for an INVITE where the UE did not detect that an emergency number had been dialled, the UE initiates a CS emergency call in supported CS domain over UTRAN or GERAN.

19.3.2.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated EPS bearers, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell A power level is set as "serving cell" and cell 24/cell 5 power level is set as "suitable cell"

Note: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure

1-2) MO call is initiated on the UE by dialling a non emergency number. UE sends INVITE REQUEST.

3) SS responds to the INVITE request with a 380 Alternative Service.

4) UE ACKs the 380 Alternative Service. UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS emergency call with MM/GMM registration if necessary.

5) CS emergency call is established and released. For GERAN cell, UE performs MM/GMM registration after CS call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates a normal call	MO call is initiated on the UE by dialling a “non emergency” number.
2	→		INVITE	UE sends INVITE. Request-URI of the INVITE request matches with the “non emergency” number dialled.
3	←		380 Alternative Service	The SS responds with a 380 Alternative Service
4	→		ACK	The UE acknowledges the receipt of 380 Alternative Service for INVITE NOTE 1: Step 4 can happen in parallel to step 4Aa1.
			EXCEPTION: The UE performs a domain selection for the emergency call and within 2 seconds of step 3 the UE may transmit EXTENDED SERVICE REQUEST	NOTE 2: Value of 2 seconds is based on estimation.
4Aa1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
4Aa2	<-		SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
5a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN) and performs emergency call in CS domain together with MM/GMM registration	NOTE 3: RAU procedure can take place in parallel to emergency CS call.
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration/deregistration defined in Annex C.46/C.30 of TS 34.229-1 can take place	
5a2			SS configures cell A as a “non-suitable cell”	
5a3			Emergency CS call is released	
5b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs CS fallback or cell reselection to a cell supporting CS domain (GERAN cell) and performs emergency call in CS domain	
5b2			SS configures cell A as a “non-suitable cell”	
5b3			Emergency CS call is released	
5b4			UE performs MM/GMM registration	

NOTE: The default messages contents in annex A are used with condition “IMS security “ or “GIBA” when applicable.

Specific Message Contents

ATTACH ACCEPT (preamble)

Use the default message as in TS 36.508 [94] sub-clause Table 4.7.2-1 except the following change:

Information Element	Value/remark	Comment
EPS network feature support	'0000 0001'B	IMS voice over PS session in S1 mode supported emergency bearer services in S1 mode not supported

INVITE (Step 2)

Use the default message “INVITE” in annex A.2.1 for MO Call” in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c*=*IN* (addrtype) (connection-address for UE) [Note 1] Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c*=*IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec shall be present

380 Alternative Service (Step 3)

Use the default message “380 Alternative Service” in annex A.4.1 with the following exceptions:

Header/param	Value/Remark
Contact	
Name-addr	urn:service:sos

ACK (Step 4)

Use the default message "ACK" in annex A.2.7

RRCConnectionRelease (step 4Aa2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (step 5b4)

Use the default message with the following specific contents:

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

19.3.2.5 Test requirements

In step 5a1 or 5b1, UE initiates a CS emergency call in UTRAN or GERAN cell (respectively).

Check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 2: the UE sends an INVITE message with correct content.

Step 5a1, 5b1: Check that the emergency call on the CS domain UTRAN or GERAN is successfully established according to the procedures described in 3GPP TS 24.008 [12].

19.3.2a Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Non-emergency IMS registration / CDMA 2000 1xRTT

19.3.2a.1 Definition

Same as in 19.3.2.1, except: UE correctly requests an emergency service on CS domain over CDMA 2000 1xRTT.

19.3.2a.2 Conformance requirement

Same Conformance requirement as in clause 19.3.2.2

19.3.2a.3 Test purpose

To verify that if the UE is not able to detect that an emergency number has been dialled:

- in the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <alternative-service> child element with the <type> child element set to "emergency" and the <action> element is not set to "emergency-registration", the UE:

- send an ACK request to the P-CSCF as per normal SIP procedures;

- attempt an emergency call setup via CS domain CDMA 2000 1xRTT according to the procedures described in 3GPP2 TS C.S0005-E[112], only if the P-Asserted-Identity header field with a value equal to the value of the SIP URI of the P-CSCF received in the Path header field during registration.

19.3.2a.4 Method of test

Initial conditions

Same as in 19.3.2.4, except: UE contains ISIM and USIM and CSIM or USIM and CSIM applications on UICC.

The SS is configured:

- with 2 cells: as in TS 36.508

- E-UTRAN cell A
- 1xRTT cell 19
- Cell A power level is set as “serving cell” cell 19 power level is set as “suitable cell”

Test procedure

Same as in 19.3.2.4 except step 5:

5) SS waits for an emergency call setup according to the procedures described in 3GPP2 TS C.S0005-E[112].

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				MO call is initiated on the UE by dialling a “non emergency” number.
2	→		INVITE	UE sends INVITE. Request-URI of the INVITE request matches with the “non emergency” number dialled.
3	←		380 Alternative Service	The SS responds with a 380 Alternative Service
4	→		ACK	The UE acknowledges the receipt of 380 response for INVITE and starts the emergency call in CS domain
5				SS waits for an emergency call setup. according to the procedures described in 3GPP2 TS C.S0005-E[112].
6				Having reached the active state, the call is cleared by the SS

NOTE: The default messages contents in annex A are used with condition “IMS security “ or “GIBA ” when applicable.

Specific Message Contents

Same as in 19.3.2.4

19.3.2a.5 Test requirements

Same as 19.3.2.5.

Except Steps 5, 6: SS must check that the emergency call on the CS domain CDMA 2000 1xRTT is successfully established according to the procedures described in 3GPP TS 24.008 [12].

19.3.2b Non-UE detectable emergency call / IM CN sends a 380 with unavailable emergency service URN / UE performs normal call via CS domain / UTRAN or GERAN

19.3.2b.1 Definition

Test to verify that the UE correctly requests normal voice service on CS domain over UTRAN or GERAN if the UE has received a 380 (Alternative Service) response to an INVITE request with Contact header field which does not match any emergency service URN.

19.3.2b.2 Conformance requirement

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN does not define emergency bearers, the UE shall attempt an emergency call as described in subclause 5.1.6.8.4.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN defines emergency bearers and the core network has indicated that it supports emergency bearers, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is not currently registered, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is attached to a different network than its home operator's network (e.g. VPLMN), the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

The IP-CAN can, dependent on the IP-CAN capabilities, provide local emergency numbers (including information about emergency service categories) to the UE which has that capability, in order for the UE to recognize these numbers as emergency call.

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

...

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

  - the first entry in the list of public user identities provisioned in the UE;

  - the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and

  - the derived temporary public user identity, in all other cases.

[TS 24.229 clause 5.1.6.8.1]:

The UE shall translate any user indicated emergency number as specified in 3GPP TS 22.101 [1A] to an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69].

When an initial request for a dialog or a standalone transaction, or an unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 is initiated:

- in event other than reception of a 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4; or

- upon reception of a 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4, and the 380 (Alternative Service) response does not contain a Contact header field containing a service URN with a top-level service type of "sos",

the Request-URI of the initial request for a dialog or the standalone transaction, or the unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 shall include one of the following service URNs; "urn:service:sos", "urn:service:sos.ambulance", "urn:service:sos.police", "urn:service:sos.fire", "urn:service:sos.marine", "urn:service:sos.mountain". If the UE can determine the type of emergency service the UE shall use an emergency service URN with a sub-service type corresponding to the type of emergency service.

NOTE 1: A service URN with a top-level service type of "sos" is used only when the user intends to establish an emergency call.

When an initial request for a dialog or a standalone transaction, or an unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 is initiated upon reception of 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4, and if the 380 (Alternative Service) response contains a Contact header field containing a service URN with a top-level service type of "sos", the UE shall set the Request-URI of the initial request for a dialog or the standalone transaction, or the unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 to the service URN of the Contact header field of the 380 (Alternative Service) response.

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response including a 3GPP IM CN subsystem XML body as described in subclause 7.6 that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), the UE shall automatically send an ACK request to the P-CSCF as per normal SIP procedures and terminate the session. In addition, if the 380 (Alternative Service) response includes a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration:

- the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element; and

- one of subclause 5.1.6.8.3 or subclause 5.1.6.8.4 applies.

NOTE 2: Emergency numbers which the UE does not detect, will be treated as a normal call.

NOTE 3: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A and 5.1.3 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a service URN in the Request-URI of the INVITE request in accordance with subclause 5.1.6.8.1;

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 1: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

- if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

In the event the UE receives a 380 (Alternative Service) response with a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration, and the Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the following treatment is applied:

1) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), then the UE shall:

a) if the CS domain is available to the UE, and no prior attempt using the CS domain for the current emergency call attempt has been made, attempt emergency call via CS domain using appropriate access technology specific procedures;

b) if the CS domain is not available to the UE or the emergency call has already been attempted using the CS domain, then perform one of the following actions:

- if the <action> child element of the <alternative-service> child element of the <ims-3gpp> element in the IM CN subsystem XML body as described in subclause 7.6 is set to "emergency-registration" (see table 7.6.3), perform an initial emergency registration using a different VPLMN if available, as described in subclause 5.1.6.2 and if the new emergency registration succeeded, attempt an emergency call as described in this subclause; or

- perform implementation specific actions to establish the emergency call; and

2) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2) then the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 4: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

[TS 24.229 annex L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

…

NOTE 1: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] will be considered as a visited network.

The type of emergency service for an emergency number is derived from the settings of the emergency service category value (bits 1 to 5 of the emergency service category value as specified in subclause 10.5.4.33 of 3GPP TS 24.008 [8]). Table L.2.2.6.1 below specifies mappings between a type of emergency service and an emergency service URN. The UE shall use the mapping to match an emergency service URN and a type of emergency service. If a dialled number is an emergency number but does not map to a type of emergency service the service URN shall be "urn:service:sos".

Table L.2.2.6.1: Mapping between type of emergency service and emergency service URN

Type of emergency service	Emergency service URN
Police	urn:service:sos.police
Ambulance	urn:service:sos.ambulance
Fire Brigade	urn:service:sos.fire
Marine Guard	urn:service:sos.marine
Mountain Rescue	urn:service:sos.mountain

Upon reception of a 380 (Alternative Service) response to an INVITE request as defined in subclause 5.1.2A.1.1 and subclause 5.1.3.1, if:

- the 380 (Alternate Service) response contains a Contact header field;

- the value of the Contact header field is a service URN; and

- the service URN has a top-level service type of "sos";

then the UE determines that "emergency service information is included" as described 3GPP TS 23.167 [4B], else the UE determines that "emergency service information" as described 3GPP TS 23.167 [4B] is not included.

If the "emergency service information is included" as described 3GPP TS 23.167 [4B]:

1) if the URN in the Contact header field matches an emergency service URN in table L.2.2.6.1, then the type of emergency service is the value corresponding to the matching entry in table L.2.2.6.1; and

2) if the URN in the Contact header field does not match any emergency service URN in table L.2.2.6.1, then the type of emergency service is not identified.

NOTE 3: In bullet 2), the URN in the Contact header field either contains "no emergency subservice type" as described in 3GPP TS 23.167 [4B] triggering an emergency call, or contains an "emergency subservice type that does not map into an emergency service category for the CS domain" as described in 3GPP TS 23.167 [4B] triggering a normal call when the dialled number is available or triggering an emergency call when the dialled number is not available. The country specific URN is an example of a "emergency subservice type that does not map into an emergency service category for the CS domain".

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.31, 5.1.6.8.3 and Annex L2.2.6 (release 9)

19.3.2b.3 Test purpose

1) To verify that the on reception of 380 Alternate Service with Contact header field which does not match any emergency service URN specified in TS 24.229 [10] for an INVITE sent for emergency call establishment, UE initiates the normal call in supported CS domain over UTRAN or GERAN.

19.3.2b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN , GERAN cell 24
- Cell A power level is set as “serving cell” and cell 24/cell 5 power level is set as “suitable cell”

NOTE: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-2) MO call is initiated on the UE by dialling a non emergency number.

3) SS responds with 380 Alternative services.

4) UE ACKS the 380 Alternative service message.

5) UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain normal call with MM/GMM registration if necessary.

6) CS call is established.

7) CS call is released. For GERAN cell, UE performs MM/GMM registration after CS call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates a normal call	MO call is initiated on the UE by dialling a "non emergency" number.
2	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports
3	←		380 Alternative Service	The SS responds with a 380 Alternative Service response
4	→		ACK	The UE acknowledges the receipt of 380 Alternative Service for INVITE NOTE 1: Step 4 can happen in parallel to step 4Aa1.
			EXCEPTION: The UE performs a domain selection for the emergency call and within 2 seconds of step 3 the UE may transmit EXTENDED SERVICE REQUEST	NOTE 2: Value of 2 seconds is based on estimation.
4Aa1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback* as defined in 24.301 clause 9.9.3.27
4Aa2	<-		SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
			EXCEPTION: Either step 5a1 or 5b1 is performed, depending on the value of px_RATComb_Tested	
5a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN) and performs normal call in CS domain together with MM/GMM registration	NOTE 3: RAU procedure can take place in parallel to normal CS call.
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration/deregistration defined in Annex C.46/C.30 of TS 34.229-1 can take place	
5a2			SS configures cell A as a "non-suitable cell"	
5a3			Normal CS call is released	
5b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs CS fallback or cell reselection to a cell supporting CS domain (GERAN cell) and performs normal call in CS domain	
5b2			SS configures cell A as a "non-suitable cell"	
5b3			Normal CS call is released	
5b4			UE performs MM/GMM registration	

Specific Message Contents

ATTACH ACCEPT (preamble)

Use the default message as in TS 36.508 [94] sub-clause Table 4.7.2-1 except the following change:

Information Element	Value/remark	Comment
EPS network feature support	'0000 0001'B	IMS voice over PS session in S1 mode supported emergency bearer services in S1 mode not supported

380 Alternative Service (Step 3)

Use the default message "380" in annex A.4.1 with the following exceptions:

Header/param	Value/Remark
Contact	
Name-addr	urn:service:sos.country-specific

RRCConnectionRelease (step 4Aa2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (step 5b4)

Use the default message with the following specific contents:

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

19.3.2b.5 Test requirements

In step 5a1 or 5b1, UE initiates a CS normal call in UTRAN or GERAN cell (respectively).

19.3.2c Non-UE detectable emergency call / IM CN sends a 380 with available emergency service URN / UE performs CS Emergency call via CS domain / UTRAN or GERAN

19.3.2c.1 Definition

Test to verify that the UE correctly requests CS emergency voice service on CS domain over UTRAN or GERAN if the UE has received a 380 (Alternative Service) response to an INVITE request with Contact header field which matches an emergency service URN.

19.3.2c.2 Conformance requirement

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN does not define emergency bearers, the UE shall attempt an emergency call as described in subclause 5.1.6.8.4.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN defines emergency bearers and the core network has indicated that it supports emergency bearers, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is not currently registered, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is attached to a different network than its home operator's network (e.g. VPLMN), the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

The IP-CAN can, dependent on the IP-CAN capabilities, provide local emergency numbers (including information about emergency service categories) to the UE which has that capability, in order for the UE to recognize these numbers as emergency call.

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

...

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

 - the first entry in the list of public user identities provisioned in the UE;

 - the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and

 - the derived temporary public user identity, in all other cases.

[TS 24.229 clause 5.1.6.8.1]:

The UE shall translate any user indicated emergency number as specified in 3GPP TS 22.101 [1A] to an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69].

When an initial request for a dialog or a standalone transaction, or an unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 is initiated:

- in event other than reception of a 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4; or

- upon reception of a 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4, and the 380 (Alternative Service) response does not contain a Contact header field containing a service URN with a top-level service type of "sos",

the Request-URI of the initial request for a dialog or the standalone transaction, or the unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 shall include one of the following service URNs; "urn:service:sos", "urn:service:sos.ambulance", "urn:service:sos.police", "urn:service:sos.fire", "urn:service:sos.marine", "urn:service:sos.mountain". If the UE can determine the type of emergency service the UE shall use an emergency service URN with a sub-service type corresponding to the type of emergency service.

NOTE 1: A service URN with a top-level service type of "sos" is used only when the user intends to establish an emergency call.

When an initial request for a dialog or a standalone transaction, or an unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 is initiated upon reception of 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4, and if the 380 (Alternative Service) response contains a Contact header field containing a service URN with a top-level service type of "sos", the UE shall set the Request-URI of the initial request for a dialog or the standalone transaction, or the unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 to the service URN of the Contact header field of the 380 (Alternative Service) response.

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response including a 3GPP IM CN subsystem XML body as described in subclause 7.6 that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), the UE shall automatically send an ACK request to the P-CSCF as per normal SIP procedures and terminate the session. In addition, if the 380 (Alternative Service) response includes a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration:

- the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element; and

- one of subclause 5.1.6.8.3 or subclause 5.1.6.8.4 applies.

NOTE 2: Emergency numbers which the UE does not detect, will be treated as a normal call.

NOTE 3: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A and 5.1.3 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a service URN in the Request-URI of the INVITE request in accordance with subclause 5.1.6.8.1;

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 1: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

   - if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

In the event the UE receives a 380 (Alternative Service) response with a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration, and the Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the following treatment is applied:

1) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), then the UE shall:

   a) if the CS domain is available to the UE, and no prior attempt using the CS domain for the current emergency call attempt has been made, attempt emergency call via CS domain using appropriate access technology specific procedures;

   b) if the CS domain is not available to the UE or the emergency call has already been attempted using the CS domain, then perform one of the following actions:

      - if the <action> child element of the <alternative-service> child element of the <ims-3gpp> element in the IM CN subsystem XML body as described in subclause 7.6 is set to "emergency-registration" (see table 7.6.3), perform an initial emergency registration using a different VPLMN if available, as described in subclause 5.1.6.2 and if the new emergency registration succeeded, attempt an emergency call as described in this subclause; or

      - perform implementation specific actions to establish the emergency call; and

2) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2) then the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 4: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

[TS 24.229 annex L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

…

NOTE 1: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] will be considered as a visited network.

The type of emergency service for an emergency number is derived from the settings of the emergency service category value (bits 1 to 5 of the emergency service category value as specified in subclause 10.5.4.33 of 3GPP TS 24.008 [8]). Table L.2.2.6.1 below specifies mappings between a type of emergency service and an emergency service URN. The UE shall use the mapping to match an emergency service URN and a type of emergency service. If a dialled number is an emergency number but does not map to a type of emergency service the service URN shall be "urn:service:sos".

Table L.2.2.6.1: Mapping between type of emergency service and emergency service URN

Type of emergency service	Emergency service URN
Police	urn:service:sos.police
Ambulance	urn:service:sos.ambulance
Fire Brigade	urn:service:sos.fire
Marine Guard	urn:service:sos.marine
Mountain Rescue	urn:service:sos.mountain

Upon reception of a 380 (Alternative Service) response to an INVITE request as defined in subclause 5.1.2A.1.1 and subclause 5.1.3.1, if:

- the 380 (Alternate Service) response contains a Contact header field;
- the value of the Contact header field is a service URN; and
- the service URN has a top-level service type of "sos";

then the UE determines that "emergency service information is included" as described 3GPP TS 23.167 [4B], else the UE determines that "emergency service information" as described 3GPP TS 23.167 [4B] is not included.

If the "emergency service information is included" as described 3GPP TS 23.167 [4B]:

1) if the URN in the Contact header field matches an emergency service URN in table L.2.2.6.1, then the type of emergency service is the value corresponding to the matching entry in table L.2.2.6.1; and
2) if the URN in the Contact header field does not match any emergency service URN in table L.2.2.6.1, then the type of emergency service is not identified.

NOTE 3: In bullet 2), the URN in the Contact header field either contains "no emergency subservice type" as described in 3GPP TS 23.167 [4B] triggering an emergency call, or contains an "emergency subservice type that does not map into an emergency service category for the CS domain" as described in 3GPP TS 23.167 [4B] triggering a normal call when the dialled number is available or triggering an emergency call when the dialled number is not available. The country specific URN is an example of a "emergency subservice type that does not map into an emergency service category for the CS domain".

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.31, 5.1.6.8.3 and Annex L2.2.6 (release 9)

19.3.2c.3 Test purpose

1) To verify that on reception of 380 Alternate Service with Contact header field which matches an emergency service URN specified in TS 24.229 [10] for an INVITE sent for emergency call establishment, UE initiates the CS emergency call in supported CS domain over UTRAN or GERAN.

19.3.2c.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN , GERAN cell 24
- Cell A power level is set as “serving cell” and cell 24/cell 5 power level is set as “suitable cell”

NOTE: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-2) MO call is initiated on the UE by dialling a non emergency number.

3) SS responds with 380 Alternative services.

4) UE ACKS the 380 Alternative service message.

4A and 4B) UE may initiate CS fallback. If so SS releases the RRC connection.

5) UE performs cell reselection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM/GMM registration if necessary. Emergency CS call is released. For GERAN cell, UE performs MM/GMM registration after emergency CS call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates a normal call	MO call is initiated on the UE by dialling a "non emergency" number.
2	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports
3	←		380 Alternative Service	The SS responds with a 380 Alternative Service response
4	→		ACK	The UE acknowledges the receipt of 380 Alternative Service for INVITE NOTE 1: Step 4 can happen in parallel to step 4A.
			EXCEPTION: The UE performs a domain selection for the emergency call and within 2 seconds of step 3 the UE may transmit EXTENDED SERVICE REQUEST	NOTE 2: Value of 2 seconds is based on estimation.
4Aa1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends Extended service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
4Aa2	←		SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported) NOTE 3: This step happens only if step 4Aa1 was performed
			EXCEPTION: Either step 5a1 or 5b1 is performed, depending on the value of px_RATComb_Tested	
5a1			I IF px_RATComb_Tested = EUTRA_UTRA UE performs cell reselection to a cell supporting CS domain (UTRAN cell) and performs emergency call in CS domain after together with MM/GMM registration (if needed)	NOTE 4: RAU procedure can take place in parallel to emergency CS call.
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration/deregistration defined in Annex C.46/C.30 of TS 34.229-1 can take place	
5a2			SS configures cell A as a "non-suitable cell"	
5a3			Emergency CS call is released	
5b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs cell reselection to a cell supporting CS domain (GERAN cell) and performs emergency call in CS domain	
5b2			SS configures cell A as a "non-suitable cell"	
5b3			Emergency CS call is released	
5b4			UE performs MM/GMM registration	

Specific Message Contents

ATTACH ACCEPT (preamble)

Use the default message as in TS 36.508 [94] sub-clause Table 4.7.2-1 except the following change:

Information Element	Value/remark	Comment
EPS network feature support	'0000 0001'B	IMS voice over PS session in S1 mode supported emergency bearer services in S1 mode not supported

380 Alternative Service (Step 3)

Use the default message "380" in annex A.4.1 with the following exceptions:

Header/param	Value/Remark
Contact	
Name-addr	urn:service:sos.police

RRCConnectionRelease (step 4Aa2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (Step 5b4)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

19.3.2c.5 Test requirements

In step 5a1 or 5b1, the UE initiates a CS emergency call in UTRAN or GERAN cell (respectively).

19.3.3 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Emergency IMS registration

19.3.3.1 Definition

To verify that a UE issuing a non-UE detectable emergency call and receiving a 380 Alternative Service response will perform emergency registration and start an emergency call then.

19.3.3.2 Conformance requirement

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency", the UE shall attempt an emergency call.

NOTE 11: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

...

When an initial request for a dialog or a standalone transaction, or an unknown method transmitted as part of UE detected emergency call procedures is initiated upon reception of 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method, and if the 380 (Alternative Service) response contains a Contact header field containing a service URN with a top-level service type of "sos", the UE shall set the Request-URI of the initial request for a dialog or the standalone transaction, or the unknown method transmitted as part of UE detected emergency call procedures to the service URN of the Contact header field of the 380 (Alternative Service) response.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.3.1 and 5.1.6.8.1.

19.3.3.3 Test purpose

1) To verify that when a UE issuing a non-UE detectable emergency call and receiving a 380 Alternative Service response will perform emergency registration and then start an emergency call; and

2) To verify that the UE will correctly populate SIP headers and bodies.

19.3.3.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated EPS bearers, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

1-2) MO call is initiated on the UE by dialling a non emergency number.

3) SS responds to the INVITE request with a 380 Alternative Service.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 380 Alternative Service.

5-11) SS waits for an IMS emergency registration and call setup.

12-19) Void.

20-21) Having reached the active state, the call is cleared by the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				MO call is initiated on the UE by dialling a “non emergency” number.
2	→		INVITE	UE sends INVITE. Request-URI of the INVITE request matches with the “non emergency” number dialled.
3	←		380 Alternative Service	The SS responds with a 380 Alternative Service
			EXCEPTION: Step 4 and Steps 5-13 may occur in parallel	
4	→		ACK	The UE acknowledges the receipt of 380 response for INVITE.
5-13			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1, steps 9-15, for a UE with E-UTRA support, see NOTE 2.
14-19				Void
20	→		BYE	The UE releases the call with BYE
21	←		200 OK	The SS sends 200 OK for BYE

NOTE 1: The default messages contents in annex A are used with condition "IMS security".

NOTE 2: After step 4, an RRC connection already exists. Therefore the UE will directly send PDN CONNECTIVITY REQUEST for emergency bearer without service request procedure. Hence, 36.508 table 4.5A.4.3-1 steps 9-15 will be executed.

Specific Message Contents

INVITE (Step 2 of Annex C.21)

Use the default message “INVITE” in annex A.2.1. for MO Call” in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec shall be present

380 Alternative Service (Step 3)

Use the default message “380 Alternative Service” in annex A.4.1 with the following exception.

Header/param	Value/remark	Rel	Reference
Contact			
addr-spec	*urn:service:sos.ambulance*		
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>emergency</type>* *<reason/>* *<action>*emergency-registration</action> *</alternative-service>* *</ims-3gpp>*		

ACK (Step 4)

Use the default message "ACK" in annex A.2.7

INVITE (step 1 of Annex C.22)

Use the default message “INVITE for MO call setup” in annex A.2.1. with conditions A7 and A8 and the following exceptions:

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				
Request-URI		*urn:service:sos.ambulance*		

180 Ringing for INVITE (step 3 of Annex C.22)

Use the default message “180 Ringing for INVITE” in annex A.2.6. The condition A4 “180 sent by the SS when setting up an emergency call” shall apply.

200 OK for INVITE (step 4 of Annex C.22)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1. The condition A6 “Response sent by SS for INVITE for emergency call” shall apply

BYE (Step 20)

Use the default message “BYE” in annex A.2.8.

19.3.3.5 Test requirements

Steps 5-11: the UE sets up emergency call correctly.

19.3.4 Non-UE detectable emergency call / IM CN sends 380 with an Alternative Service / Previous emergency IMS registration not expired

19.3.4.1 Definition

To verify that a UE issuing a non-UE detectable emergency call, having a non-expired IMS registration and receiving a 380 Alternative Service response will not perform emergency registration, but will start an emergency call using the non-expired IMS registration.

19.3.4.2 Conformance requirement

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp>

element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency", the UE shall attempt an emergency call.

NOTE 11: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

…

The UE shall perform a new initial emergency registration if the UE determines that:

- it has previously performed an emergency registration which has not yet expired; and
- it has obtained an IP address from the serving IP-CAN different than the IP address used for the emergency registration.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.3.1, 5.1.6.2A.

19.3.4.3 Test purpose

1) To verify that when a UE issuing a non-UE detectable emergency call, having a non-expired IMS registration and receiving a 380 Alternative Service response will not perform emergency registration, but will start an emergency call using the non-expired IMS registration; and

2) To verify that the UE will correctly populate SIP headers and bodies.

19.3.4.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated EPS bearers, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure

1-15) Emergency registration followed by an emergency call set-up

16-17) The emergency call is terminated by the UE

18) MO call is initiated on the UE by dialling a non emergency number.

19) SS waits the UE to send an INVITE request with Request-URI that matches the non emergency number dialled.

20) SS responds to the INVITE request with a 380 Alternative Service.

21) SS waits for the UE to send an ACK to acknowledge receipt of the 380 Alternative Service.

22-25) Void

26-37) SS waits for IMS Emergency Call Setup procedure

38-39) Having reached the active state, the call is cleared by the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-9			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
10-15				Void
16	→		BYE	The UE releases the call with BYE
17	←		200 OK	The SS sends 200 OK for BYE
18				MO call is initiated on the UE by dialling a “non emergency” number.
19	→		INVITE	UE sends INVITE. Request-URI of the INVITE request matches with the “non emergency” number dialled.
20	←		380 Alternative Service	The SS responds with a 380 Alternative Service
21	→		ACK	The UE acknowledges the receipt of 380 response for INVITE.
22-25				Void
26-30			Steps defined in annex C.22	IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
31-37				Void
38	→		BYE	The UE releases the call with BYE
39	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition “IMS security “.

Specific Message Contents

INVITE (Step 19)

Use the default message “INVITE” in annex A.2.1. for MO Call” in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec shall be present

380 Alternative Service (Step 20)

Use the default message “380 Alternative Service” in annex A.4.1 with the following exception.

Header/param	Value/remark	Rel	Reference
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>emergency</type>* *<reason/>* <*action*>emergency-registration</action> *</alternative-service>* *</ims-3gpp>*		

ACK (Step 21)

Use the default message "ACK" in annex A.2.7

INVITE (step 1 of Annex C.22)

Use the default message “INVITE for MO call setup” in annex A.2.1. with the following conditions:

- A7 “INVITE for creating an emergency session within an emergency registration” shall apply; and
- A8 “UE uses Geolocation header to provide its geographical location for emergency session setup, has obtained its location and is setting up an emergency session “ shall apply if the UE uses Geolocation header to provide its geographical location for emergency session setup.

180 Ringing for INVITE (step 3 of Annex C.22)

Use the default message “180 Ringing for INVITE” in annex A.2.6. The condition A4 “180 sent by the SS when setting up an emergency call” shall apply.

200 OK for INVITE (step 4 of Annex C.22)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1. The condition A6 “Response sent by SS for INVITE for emergency call” shall apply

BYE (Steps 16, 38)

Use the default message “BYE” in annex A.2.8.

19.3.4.5 Test requirements

Steps 26-30: the UE sets up emergency call correctly.

19.4 Emergency session set-up in case of no registration

19.4.1 Emergency call without emergency registration / EPS / UE does not contain an ISIM or USIM

19.4.1.1 Definition

Test to verify that the UE can initiate an IMS emergency call when the UE does not contain ISIM or USIM.

19.4.1.2 Conformance requirement

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.1 and 5.1.6.8.2.

[TS 24.229 clause 5.1.6.1]

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

[TS 24.229 clause 5.1.6.8.2]

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261.

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261;

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depend on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in draft-ietf-sipcore-keep;

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available, the UE shall include the location information in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, in accordance with RFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, in accordance with RFC 6442 [98]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 5: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

19.4.1.3 Test purpose

1) To verify that the UE is able to request activation of EPS emergency bearer contexts, according to 3GPP TS 24.229 [10] 5.1.6.1; and

2) To verify that the UE sends a correctly composed SIP INVITE request for the emergency call setup and will correctly complete the emergency session setup, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.2 and 6.1.2.

19.4.1.4 Method of test

Initial conditions

The UE is Switched OFF and contains no ISIM or USIM.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-19) UE executes the procedures described in TS 36.508 [94] table 4.5A.5.3-1 steps 1 to 19 for EPS emergency bearer context activation and subsequent IMS emergency speech call.

Expected sequence:

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-5			Steps defined in annex C.22	Generic test procedure for setting up emergency speech call. Referred from 36.508 [94] table 4.5A.5.3-1 for a UE with E-UTRA support.
6			Void	
7			Void	
8-12			Steps defined in annex C.32	UE releases the emergency call using generic test procedure for MO release of IMS call

Specific Message Contents

INVITE (Step 1)

Use the default message “INVITE for MO call setup” in annex A.2.1. with the following conditions:

- A6 “INVITE for creating an emergency session in case of no registration” shall apply; and
- A8 “UE is capable of obtaining location information, has obtained its location and is setting up an emergency session “ shall apply if the UE is capable of obtaining location information.

19.4.1.5 Test requirements

The UE shall send requests and responses as described in clause 19.4.1.4.

19.4.2 Emergency call without emergency registration / EPS / UE contains an ISIM or USIM / UE is in state EMM-REGISTERED.LIMITED-SERVICE

19.4.2.1 Definition

Test to verify that the UE with ISIM or USIM and in state EMM-REGISTERED.LIMITED-SERVICE, establishes an emergency call if emergency call is initiated. The process consists of setting the emergency call without IMS emergency registration.

19.4.2.2 Conformance requirement

[TS 24.229 clause L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

Some jurisdictions allow emergency calls to be made when the UE does not contain an ISIM or USIM, or where the credentials are not accepted. Additionally where the UE is in state EMM-REGISTERED.LIMITED-SERVICE and EMM-REGISTERED.PLMN-SEARCH, a normal ATTACH has been attempted and it can also be assumed that a registration in the IM CN subsystem will also fail. In such cases, the procedures for emergency calls without registration apply, as defined in subclause 5.1.6.8.2.

[TS 24.229 clause 5.1.6.8.2]:

When establishing an emergency session for an unregistered user, the UE is allowed to receive responses to emergency requests and requests inside an established emergency session on the unprotected ports. The UE shall reject or silently discard all other messages not arriving on a protected port. Additionally, the UE shall transmit signalling packets pertaining to the emergency session from the same IP address and unprotected port on which it expects to receive signalling packets containing the responses to emergency requests and the requests inside the established emergency session.

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261 [26].

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depend on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in draft-ietf-sipcore-keep [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available, the UE shall include the location information in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, in accordance with RFC 6442 [98]; or

   - if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, in accordance with RFC 6442 [98]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 5: It is an implementation option whether these actions are also triggered by other means.

NOTE 6: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

NOTE 7: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

If the response for the initial INVITE request indicates that the UE is behind NAT, and the INVITE request was sent over TCP connection, the UE shall keep the TCP connection during the entire duration of the emergency session. In this case the UE will receive all responses to the emergency requests and the requests inside the established emergency session over this TCP connection.

If the Via header field of any provisional response, or of the final 200 (OK) response, for the initial INVITE request contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, the UE shall start to send keep-alives associated with the session towards the P-CSCF, as described in draft-ietf-sipcore-keep [143].

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.8.2 and Annex L2.2.6 (release 9)

19.4.2.3 Test purpose

1) To verify that the UE in state EMM-REGISTERED.LIMITED-SERVICE, on initiation of an emergency call, performs EMM emergency registration to acquire a local IP address, discover a P-CSCF, and establishes an IP-CAN bearer that can be used for SIP signalling and then composes an INVITE request for the emergency call setup and will correctly complete the emergency session setup.

19.4.2.4 Method of test

Initial conditions

The UE contains either ISIM and USIM applications or only USIM application on UICC. The UE is initially IMS registered in cell A and made to select cell B. The Tracking area update procedure is rejected with cause #15, No suitable cells in tracking area in cell B, thus ensuring that the UE is in state EMM-REGISTERED.LIMITED-SERVICE.

The SS is configured with the IMSI within the USIM application, the home domain name, the SS is listening to SIP default port 5060 for both UDP and TCP protocols. The SS supports EMM emergency attach procedure and emergency bearers.

The SS configures two cells as below:

EUTRA cell A and Cell B as in TS 36.508

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

- the IMS emergency call is initiated on the UE.
- UE executes the procedures described in TS 36.508 [94] table 4.5A.5.3-1 steps 1 to 19 for EMM Emergency registration, EPS emergency bearer context activation, IMS emergency speech call establishment with PSAP.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-6			Steps defined in annex C.22	Generic test procedure for setting up emergency speech call. Referred from 36.508 [94] table 4.5A.5.3-1 for a UE with E-UTRA support.
6A-C			Steps 1-3 of Annex C.32	The UE releases the emergency call using steps 1-3 of Annex C.32
7			void	
8			void	
			EXCEPTION: Either step 9 or steps 10-11 are performed, depending on UE behaviour: if UE detaches, step 9 is performed. Otherwise, steps 10-11 are performed.	
9			Detach procedure initiated by the UE	Generic test procedure for UE initiated detach according to TS 36.508 [94] table 6.4.3.14-1 may happen within 5 seconds.
10-11			Steps 4-5 of Annex C.32	If step 9 was not performed steps 4-5 of Annex C.32 are performed

Specific Message Contents

INVITE (step 1 of procedure in annex C.22)

Use the default message “INVITE for MO call setup” in annex A.2.1 with the following conditions:

- A6 “INVITE for creating an emergency session in case of no registration” shall apply;

19.4.2.5 Test requirements

In steps 2-6, UE establishes an emergency call.

19.4.3 Void

19.4.4 Void

19.4.5 Emergency call without emergency registration / UE credentials are not accepted

19.4.5.1 Definition

Test to verify that when UE is unable to emergency register due to UE credentials not accepted, initiates an emergency call on non protected ports when an emergency call is attempted. The process consists of setting up IMS emergency call after emergency registration failure.

19.4.5.2 Conformance requirement

[TS 24.229 clause 4.2B]:

In case of an emergency session if the UE does not have sufficient credentials to authenticate with the IM CN subsystem and regulations allow, the UE and P-CSCF shall send request and responses other than initial REGISTER requests on non protected ports.

[TS 24.229 clause 4.7]:

The need for support of emergency calls in the IM CN subsystem is determined by national regulatory requirements.

If the UE cannot detect the emergency call attempt, the UE initiates the request as per normal procedures as described in subclause 5.1.2A. Depending on network policies, for a non-roaming UE an emergency call attempt can succeed even if the UE did not detect that an emergency session is being requested, otherwise the network rejects the request indicating to the UE that the attempt was for an emergency service.

The UE procedures for UE detectable emergency calls are defined in subclause 5.1.6.

The P CSCF, S-CSCF, and E-CSCF procedures for emergency service are described in subclause 5.2.10, 5.4.8 and 5.11, respectively.

Access dependent aspects of emergency service (e.g. emergency registration support and location provision) are defined in the access technology specific annexes for each access technology.

There are a number of variants within these procedures and which variant gets used depends on a number of issues. These conditions are defined more specifically in 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex, but are summarised as follows:

a) if the UE knows that it is in its own home network, then an existing registration is permitted to be used for signalling the emergency call, except where item c) applies. The access technology specific annexes define the mechanism by which home network determination is made;

b) if emergency calls are permitted without security credentials (or additionally where the authentication is not possible or has failed), then the emergency call is made directly without use of any security association created by a registration, and therefore without the registration; and

c) where the access technology defines emergency bearers for the support of emergency calls, a new emergency registration is required so that these emergency bearers can be used for both signalling and media, unless an existing emergency registration exists on those emergency bearers.

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN does not define emergency bearers, or the IP-CAN does define emergency bearers but the core network has not indicated that it supports emergency bearers, the UE shall attempt an emergency call as described in subclause 5.1.6.8.4.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN defines emergency bearers and the core network has indicated that it supports emergency bearers, the UE shall:

1) perform an initial emergency registration as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is not currently registered, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is attached to a different network than its home operator's network (e.g. VPLMN), the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

The IP-CAN can, dependant on the IP-CAN capabilities, provide local emergency numbers to the UE which has that capability, in order for the UE to recognize these numbers as emergency call.

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN does not define emergency bearers, the UE shall attempt an emergency call as described in subclause 5.1.6.8.4.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN defines emergency bearers and the core network has indicated that it supports emergency bearers, the UE shall:

1) perform an initial emergency registration as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is not currently registered, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is attached to a different network than its home operator's network (e.g. VPLMN), the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

The IP-CAN can, dependent on the IP-CAN capabilities, provide local emergency numbers (including information about emergency service categories) to the UE which has that capability, in order for the UE to recognize these numbers as emergency call.

[TS 24.229 clause 5.1.6.8.2]:

When establishing an emergency session for an unregistered user, the UE is allowed to receive responses to emergency requests and requests inside an established emergency session on the unprotected ports. The UE shall reject or silently discard all other messages not arriving on a protected port. Additionally, the UE shall transmit signalling packets pertaining to the emergency session from the same IP address and unprotected port on which it expects to receive signalling packets containing the responses to emergency requests and the requests inside the established emergency session.

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261 [26].

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depend on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in draft-ietf-sipcore-keep [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available, the UE shall include the location information in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, in accordance with RFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, in accordance with RFC 6442 [98]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 5: It is an implementation option whether these actions are also triggered by other means.

NOTE 6: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

NOTE 7: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

If the response for the initial INVITE request indicates that the UE is behind NAT, and the INVITE request was sent over TCP connection, the UE shall keep the TCP connection during the entire duration of the emergency session. In this case the UE will receive all responses to the emergency requests and the requests inside the established emergency session over this TCP connection.

If the Via header field of any provisional response, or of the final 200 (OK) response, for the initial INVITE request contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, the UE shall start to send keep-alives associated with the session towards the P-CSCF, as described in draft-ietf-sipcore-keep [143].

[TS 24.229 clause 5.1.1.5.3]:

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no "auts" Authorization header field parameter and an empty "response" Authorization header field parameter, i.e. no authentication challenge response;

- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the "auts" Authorization header field parameter (see 3GPP TS 33.102 [18]).

NOTE 8: In the case of the SQN being out of range, a "response" Authorization header field parameter can be included by the UE, based on the procedures described in RFC 3310 [49].

Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing set of security associations, if available (see 3GPP TS 33.203 [19]);

- populate a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the parameters needed for the new security association setup; and

- not create a temporary set of security associations.

On receiving a 420 (Bad Extension) in which the Unsupported header field contains the value "sec-agree" and if the UE supports GPRS-IMS-Bundled authentication, the UE shall initiate a new authentication attempt with the GPRS-IMS-Bundled authentication procedures as specified in subclause 5.1.1.2.6.

[TS 24.229 clause 5.1.1.5.12]:

A UE shall only respond to two consecutive invalid challenges and shall not automatically attempt authentication after two consecutive failed attempts to authenticate. The UE may attempt to register with the network again after an implementation specific time.

Reference(s)

3GPP TS 24.229 [10], clauses 4.2A, 4.7, 5.1.6.1, 5.1.6.8.2, 5.1.1.5.3 and 5.1.1.5.12.

19.4.5.3 Test purpose

1) To verify that when not registered to IMS emergency services the UE is able to request activation of EPS emergency bearer contexts, according to 3GPP TS 24.229 [10] annex L.2.2.6; and

2) To verify that the UE sends a correctly composed initial REGISTER request for emergency services to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.6.1; and

3) To verify that the on emergency registration failure, UE continues with the emergency call on non protected ports.

4) To verify that the UI sends a correctly composed INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.3 and 6.1.2.

19.4.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 and it is attached to the HPLMN E-UTRA service as provided by SS. In the attach SS has indicated that the cell supports E-UTRA emergency bearers.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test environment shall be set up to send in response to Emergency REGISTER message a 401 Unauthorized such that UE will not be able to establish temporary set of security associations.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) IMS emergency call is initiated on the UE.

2-13) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 12 (parallel behaviour steps 1) for EPS emergency bearer context activation, IMS emergency speech call establishment with PSAP

14) UE sends initial REGISTER message.

15) The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.

16) The SS waits for the UE to set up a temporary set of security associations and to send another REGISTER request, over those security associations.

17) The SS responds REGISTER message with 403 Forbidden and ignores any further REGISTER message reception.

18-22) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 13 to 15 (parallel behaviour steps 6-10) IMS emergency speech call establishment with PSAP.

23-23F) The Call is released on the UE using annex C.32a procedure which includes the Emergency Bearer context deactivation

24-25) Void

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-13			EPS emergency bearer context activation by the UE.	Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support. Steps 2-10 of the parallel behaviour in Table 4.5A.4.3-2 is replaced by below steps 14-22.
14	→		REGISTER	The UE sends initial IMS emergency registration
15	←		401 Unauthorized	
16	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
				Note: From this point onward the SS shall ignore any Registration message sent by the UE.
17	←		403 Forbidden	The SS sends this message to get the UE in a stable state.
18-22			Steps defined in annex C.22	IMS emergency call setup with PSAP (messages exchanged on non protected port). Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
23-23F	→		Steps defined in annex C.32a	The UE releases the call (messages exchanged on non protected port)
24-25			Void.	

Specific Message Contents

REGISTER (Step 14)

Use the default message “REGISTER” in annex A.1.1 with condition A1.

REGISTER (Steps 16)

Use the default message “REGISTER” in annex A.1.1 with condition A2.

INVITE (Step 18 resp step 1 of Annex C.22)

Use the default message “INVITE for MO call setup” in annex A.2.1. with the following conditions:

- A6 “INVITE for creating an emergency session in case of no registration”

180 Ringing for INVITE (Step 20 resp step 3 of Annex C.22)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following conditions:

- A4 “180 sent by the SS when setting up an emergency call or a non-UE detectable emergency call”
- A7 “Response sent by SS for emergency call without emergency registration”

200 OK for INVITE (Step 20 resp step 4 of Annex C.22)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following conditions:

- A7 “Response sent by SS for INVITE for emergency call without emergency registration”

BYE (Step 23A)

Use the default message “BYE” in annex A.2.8 with the following conditions:

- A6 “BYE for emergency call with no registration”.

19.4.5.5 Test requirements

In step 2-13 UE performs EMM emergency registration and emergency EPS bearer context.

In steps 18-22, UE establishes an emergency call.

19.4.6 Emergency call without emergency registration / Failure of registration / Rejected by 403(Forbidden)

19.4.6.1 Definition

Test to verify that the UE can initiate an IMS emergency call without emergency registration when an IMS emergency registration is rejected by the visited network with 403 (Forbidden).

19.4.6.2 Conformance requirement

[TS 24.229 Rel-8, clause 5.1.1.2.1]

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4).

[TS 24.229 Rel-14, clause 5.1.6.2]

If:

1) the UE receives a 403 (Forbidden) response to the REGISTER request for initial emergency registration containing an "sos" SIP URI parameter in the Contact header field; and

2) the response contains a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2) and <action> child element set to "anonymous-emergencycall" (see table 7.6.3);

the UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

[TS 24.229 Rel-9, clause 5.1.6.8.2]

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

NOTE 1: Other specifications make provision for emergency service identifiers, which are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depend on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in RFC 6223 [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available or a URI that points to the location information, the UE shall include a Geolocation header field in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

- if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

9) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

10) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

Reference(s)

TS 24.229 [10] clauses 5.1.1.2.1, 5.1.6.2 and 5.1.6.8.2.

19.4.6.3 Test purpose

1) To verify that after receiving a 403 (Forbidden) response the UE initiates IMS emergency call without emergency registration.

19.4.6.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the NW is VPLMN and the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1)-12) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 12 and parallel behaviour steps 1 for EPS emergency bearer context activation,

13) SS waits for the UE to send an initial REGISTER request containing “sos” SIP URI parameter in the Contact header field.

14) The SS responds to the REGISTER request with a 403 Forbidden response,

15) The SS waits for the UE to send an INVITE request.

16)-18A) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 13 to 15 and parallel behaviour Steps 2-5 defined in annex C.22 of TS 34.229-1 for IMS Emergency call for EPS is established,

19)-23B) The UE releases the call as defined in annex C.32a which includes the Emergency Bearer context deactivation.

24)-25) Void.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-12			Steps defined in TS 36.508 [94] table 4.5A.4.3-1	EPS Bearer Activation procedure and IP address allocation according TS 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
13	→		REGISTER	UE sends initial registration for IMS services.
14	←		403 Forbidden	The SS responds with a failure.
15	→		INVITE	UE sends INVITE request without emergency registration.
16-18A			Steps 2 to 5 defined in annex C.22	IMS emergency call setup with PSAP
19-23B			Steps defined in annex C.32a	The UE releases the call
24-25			Void.	

Specific Message Contents

REGISTER (Step 13)

Use the default message “REGISTER” in annex A.1.1 with condition A7 “Initial unprotected or subsequent REGISTER for emergency registration”

403 Forbidden for REGISTER (Step 14)

Use the default message “403 FORBIDDEN” in annex A.3.2 with condition A1 “IMS emergency registration for an anonymous emergency call”.

INVITE (Step 15)

Use the default message “INVITE” in annex A.2.1 with condition A6 “INVITE for creating an emergency session in case of no registration”.

BYE (Step 20)

Use the default message “BYE” in annex A.2.8 with condition A6 “BYE for emergency call with no registration”.

19.4.6.5 Test requirements

The UE shall send requests and responses as described in clause 19.4.6.4.

19.4.7 Emergency call without emergency registration / Failure of registration / against a network with GIBA support only

19.4.7.1 Definition

Test to verify that a UE not supporting GIBA can correctly initiate an IMS emergency call without emergency registration in a visited network with support for GIBA only.

19.4.7.2 Conformance requirement

[TS 24.229 Rel-8, clause 5.1.1.2.1]

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4).

[TS 24.229 Rel-14, clause 5.1.6.2]

If:

1) the UE receives a 420 (Bad Extension) response to the REGISTER request for initial emergency registration containing an "sos" SIP URI parameter in the Contact header field;

2) the UE does not support GPRS-IMS-Bundled authentication; and

3) the response contains a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2) and <action> child element set to "anonymous-emergencycall" (see table 7.6.3);

the UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

[TS 24.229 Rel-9, clause 5.1.6.8.2]

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

NOTE 1: Other specifications make provision for emergency service identifiers, which are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depend on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in RFC 6223 [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available or a URI that points to the location information, the UE shall include a Geolocation header field in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

   - if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

9) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

10) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

Reference(s)

TS 24.229 [10] clauses 5.1.1.2.1, 5.1.6.2 and 5.1.6.8.2.

19.4.7.3 Test purpose

1) To verify that after receiving a 420 (Bad Extension) response the UE initiates an IMS emergency call without emergency registration.

19.4.7.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1)-12) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 12 and parallel behaviour steps 1 for EPS emergency bearer context activation,

13) SS waits for the UE to send an initial REGISTER request containing “sos” SIP URI parameter in the Contact header field.

14) The SS responds to the REGISTER request with a 420 Bad Extension response,

15) The SS waits for the UE to send an INVITE request.

16)-18A) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 13 to 15 and parallel behaviour Steps 2-5 defined in annex C.22 of TS 34.229-1 for IMS Emergency call for EPS is established,

19)-23B) The UE releases the call as defined in annex C.32a which includes the Emergency Bearer context deactivation.

24)-25) Void.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-12			Steps defined in TS 36.508 [94] table 4.5A.4.3-1	EPS Bearer Activation procedure and IP address allocation according TS 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
13	→		REGISTER	UE sends initial registration for IMS services.
14	←		420 Bad Extension	The SS responds with a failure.
15	→		INVITE	UE sends INVITE request without emergency registration.
16-18A			Steps 2 to 5 defined in annex C.22	IMS emergency call setup with PSAP
19-23B			Steps defined in annex C.32a	The UE releases the call
24-25			Void.	

Specific Message Contents

REGISTER (Step 13)

Use the default message “REGISTER” in annex A.1.1 with condition A1 "Initial unprotected REGISTER" and A7 “Initial unprotected or subsequent REGISTER for emergency registration”

420 Bad Extension for REGISTER (Step 14)

Use the default message “420 Bad Extension for REGISTER” in annex A.1.8 with condition A1 “IMS emergency registration for an anonymous emergency call.”

INVITE (Step 15)

Use the default message “INVITE” in annex A.2.1 with condition A6 “INVITE for creating an emergency session in case of no registration”.

200 OK (Step 18)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with condition A7.

BYE (Step 20)

Use the default message “BYE” in annex A.2.8 with condition A6 “BYE for emergency call with no registration”.

19.4.7.5 Test requirements

The UE shall send requests and responses as described in clause 19.4.7.4.

19.5 Emergency registration

19.5.1 New initial emergency registration / UE obtains from the serving IP-CAN an IP address different than the IP address used for the emergency registration

19.5.1.1 Definition

Test to verify that the UE having performed emergency registration which has not yet expired, triggers a new initial emergency registration, when the UE obtains a different IP address than the one used for current emergency registration. The process consists of sending an unprotected REGISTER request for new initial emergency registration over the EPS emergency bearers, receiving 401 response, sending another REGISTER request to complete the re-authentication and receiving the 200 OK for renewed registration.

19.5.1.2 Conformance requirement

[TS 24.229 clause 5.1.6.2A]:

The UE shall perform a new initial emergency registration, as specified in subclause 5.1.6.2, if the UE determines that:

- it has previously performed an emergency registration which has not yet expired; and
- it has obtained an IP address from the serving IP-CAN, as specified in subclause 9.2.1, different than the IP address used for the emergency registration.

[TS 24.229 clause 5.1.1.2.1]:

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include an "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223 [143];

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

  1) if GRUU is supported, the option-tag "gruu"; and

  2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 4: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

a) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, the UE may initiate that mechanism on a media level when it initiates new media in an existing session.

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header field value and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 6: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;

d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 7: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 8: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626 [92], and the S-CSCF has followed the registration procedure as described in RFC 5627 [93] or RFC 3261 [26], i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626 [92], the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626 [92]; or

NOTE 9: Upon replaces the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about the deregistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626 [92];

g) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session; and

NOTE 10: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223 [143].

[TS 24.229 clause 5.1.1.4.1]:

The UE can perform the reregistration of a previously registered public user identity via an initial registration as specified in subclause 5.1.1.2, when binding the previously registered public user identity to new contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used).

... [TS 24.229 clause 5.1.1.2.2]

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

  - the "username" header field parameter, set to the value of the private user identity;

  - the "realm" header field parameter, set to the domain name of the home network;

  - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

  - the "nonce" header field parameter, set to an empty value; and

  - the "response" header field parameter, set to an empty value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the port values see 3GPP TS 33.203 [19].

b) additionally for the Contact header field, if the REGISTER request is protected by a security association, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field; and

d) a Security-Client header field set to specify the signalling plane security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203 [19], and shall announce support for them according to the procedures defined in RFC 3329 [48].

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, the UE shall additionally:

1) If the UE supports multiple registrations and the REGISTER request contained the "+sip.instance" header field parameter and the "reg-id" header field parameter in the Contact header field, and the "outbound" option-tag in the Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field. If the option-tag "outbound" is present, then the UE shall use the bidirectional flow as defined in RFC 5626 [92] as follows:

   a) for UDP, the bidirectional flow consists of two unidirectional flows, i.e. the first unidirectional flow is identified with the UE's protected client port, the P-CSCF's protected server port, and the respective IP addresses. The UE uses this flow to send the requests and responses to the P-CSCF. The second unidirectional flow is identified with the P-CSCF's protected client port, the UE's protected server port and the IP addresses. The second unidirectional flow is used by the UE to receive the requests and responses from the P-CSCF; or

   b) for TCP, the bidirectional flow is the TCP connection between the UE and the P-CSCF. This TCP connection was established by the UE, i.e. from the UE's protected client port and the UE's IP address to the P-CSCF's protected server port and the P-CSCF's IP address. This TCP connection is used to exchange SIP messages between the UE and the P-CSCF; and

2) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

NOTE 3: If the UE receives Authentication-Info, it will proceed as described in RFC 3310 [49].

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229 clause 5.1.1.5.1]:

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203;

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

   - the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

   - the "username" header field parameter, set to the value of the private user identity;

   - the "response" header field parameter that contains the RES parameter, as described in RFC 3310;

   - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

   - the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and

   - the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

   The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

[TS 33.203 clause 7.5]:

When a UE changes its IP address, e.g. by using the method described in RFC 3041 [18], then the UE shall delete the existing SA's and initiate an unprotected registration procedure using the new IP address as the source IP address in the packets carrying the REGISTER messages.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.2A, 5.1.1.2.2, 5.1.1.2.1, 5.1.1.5.1 and 5.1.6.4, 33.203 clause 7.5 (release 9).

19.5.1.3 Test purpose

1) To verify that when UE obtains an IP address different than the IP address used for current emergency registration, which is not yet expired, the UE shall perform new initial emergency registration, as defined within 3GPP TS 24.229 [10] clause 5.1.6.2A.

19.5.1.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by having executed the generic test procedure in Annex C.2 up to the last step. UE has registered to IMS emergency services, by having executed the generic test procedure in Annex C.20 up to the last step. Thereafter the UE has initiated an emergency call by having executed the generic test procedure in Annex C.22 up to the last step. The emergency call is released.

An IP address re-allocation is triggered by executing a network initiated detach procedure with detach type indication "re-attach required". The UE then triggers an Attach procedure. The SS indicates support of emergency bearers and allocates an IP address different from the one used in the attach procedure in the preamble.

Test procedure

applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call establishment with PSAP

16) Call is released on the UE. SS waits for the UE to send a BYE request.

17) SS responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-10			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
11			void	
12			void	
13-17			Steps defined in annex C.32	Make the UE release the call including EPS Bearer Deactivation procedure according to TS 36.508 [94] subclause 4.5A.15.

Specific Message Contents

INVITE (step 1 of Annex C.22)

Use the default message "INVITE for MO call setup" in annex A.2.1. with the following conditions:

- A7 "INVITE for creating an emergency session within an emergency registration" shall apply; and
- A8 "UE is capable of obtaining location information, has obtained its location and is setting up an emergency session" shall apply if the UE is capable of obtaining location information.

19.5.1.5 Test requirements

In steps 2-10 UE performs emergency EPS bearer context establishment and establishes an emergency call.

19.5.2 to 19.5.5 Void

19.5.6 User-initiated emergency reregistration / UE has emergency related ongoing dialog

19.5.6.1 Definition

Test to verify that the UE can correctly renew its emergency registration while an emergency call is going on and half of the registration time has expired. The process consists of sending a new REGISTER request over the existing security associations and EPS emergency bearers, receiving 401 response, sending another REGISTER request to complete the reauthentication and receiving the 200 OK for renewed registration.

19.5.6.2 Conformance requirement

[TS 24.229 clause 5.1.6.4]:

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if half of the time for the emergency registration has expired and:

- the UE has emergency related ongoing dialog; or
- standalone transactions exist; or
- the user initiates an emergency call.

[TS 24.229 clause 5.1.1.4.1]:

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep [143];

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174]; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep [143], towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229 clause 5.1.1.4.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter set to the value of the private user identity;

- the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;

- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

- the "nonce" header field parameter, set to last received nonce value; and

- the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 [92] and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

b) additionally for the Contact header field, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;

d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

a) set the security association lifetime associated with this contact address and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

[TS 24.229 clause 5.1.1.5.1]:

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

    - the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

    - the "username" header field parameter, set to the value of the private user identity;

    - the "response" header field parameter that contains the RES parameter, as described in RFC 3310 [49];

    - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

    - the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and

    - the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

    The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.1.4.1, 5.1.1.4.2, 5.1.1.5.1 and 5.1.6.4 (release 9)

19.5.6.3 Test purpose

1) To verify that when half of the time for the emergency registration has expired and the UE has emergency related ongoing dialog, the UE shall perform user-initiated emergency reregistration, as defined within 3GPP TS 24.229 [10] clauses 5.1.6.4, 5.1.1.4.1, 5.1.1.4.2 and 5.1.1.5.1.

19.5.6.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step. The UE has performed EPS emergency bearer context activation, IMS emergency registration and the subsequent IMS emergency call, s described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15. When performing the steps of Annex C.20 the SS sets the expiration time to 120 seconds in Step 4. Thereafter the UE has initiated an emergency call by executing the generic test procedure in Annex C.22 up to the last step.

Test procedure

1) When half of the initial emergency registration time has expired and while emergency call is still going on SS receives REGISTER request from the UE.

2) SS responds to the REGISTER request with a valid 401 Unauthorized response, headers populated according to the 401 response common message definition.

3) SS waits for the UE to set up a new set of security associations and send another REGISTER request, over those security associations.

4) The SS responds with 200 OK over the new security association, setting the new expiration time as 1200 seconds

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE re-registers to the emergency services 60 seconds before the expected expiration.
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
3	→		REGISTER	UE completes the security negotiation procedures, sets up a new temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The SS responds with 200 OK.

Specific Message Contents

REGISTER (Step 1)

Use the default message "REGISTER" in annex A.1.1. with condition A2 "Subsequent REGISTER sent over security associations" and the following exceptions applying:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and protected server port of UE. The SIP URI shall contain the *sos* URI parameter.
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous REGISTER

401 Unauthorized for REGISTER (Step 2)

Use the default message "401 Unauthorized for REGISTER" in annex A.1.2 with the following exceptions:

Header/param	Value/remark
Security-Server	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous Security-Server headers
WWW-Authenticate	
nonce	Base 64 encoding of a new RAND and AUTN

REGISTER (Step 3)

Use the default message "REGISTER" in annex A.1.1 like in step 1 above. The only difference is that the response value within Authorization header shall have been recalculated based on the nonce received from SS within 401 response.

200 OK for REGISTER (Step 4)

Use the default message "200 OK for REGISTER" in annex A.1.3 with condition A3 "Response for an emergency registration" and the expires parameter of Contact header set to 1200.

19.5.6.5 Test requirements

All the messages specified for this test case shall be sent over the EPS emergency bearers allocated for the initial emergency registration.

19.5.7 User-initiated emergency reregistration / The user initiates an emergency call

19.5.7.1 Definition

Test to verify that the UE can correctly renew its emergency registration while an emergency call is being initiated and half of the registration time has expired. The re-registration process consists of sending a new REGISTER request over the existing security associations and EPS emergency bearers, receiving 401 response, sending another REGISTER request to complete the reauthentication and receiving the 200 OK for renewed registration. The test case is applicable for IMS security.

19.5.7.2 Conformance requirement

[TS 24.229 clause 5.1.6.4]:

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if half of the time for the emergency registration has expired and:

- the UE has emergency related ongoing dialog; or
- standalone transactions exist; or
- the user initiates an emergency call.

[TS 24.229 clause 5.1.1.4.1]:

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep [143];

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174]; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep [143], towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229 clause 5.1.1.4.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter set to the value of the private user identity;
- the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to last received nonce value; and
- the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 [92] and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

b) additionally for the Contact header field, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;

d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

a) set the security association lifetime associated with this contact address and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

[TS 24.229 clause 5.1.1.5.1]:

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

   - the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

   - the "username" header field parameter, set to the value of the private user identity;

   - the "response" header field parameter that contains the RES parameter, as described in RFC 3310 [49];

   - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

   - the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and

   - the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

   The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.1.4.1, 5.1.1.4.2, 5.1.1.5.1 and 5.1.6.4 (release 9)

19.5.7.3 Test purpose

1) To verify that when half of the time for the emergency registration has expired and the UE is in the process of initiating an emergency call, the UE shall perform user-initiated emergency reregistration, as defined within 3GPP TS 24.229 [10] clauses 5.1.6.4, 5.1.1.4.1, 5.1.1.4.2 and 5.1.1.5.1.

19.5.7.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

Test procedure

Expected sequence, procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Emergency call is initiated on the UE as described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation and subsequent IMS emergency registration. The UE registers to IMS emergency services, by executing the generic test procedure in Annex C.20 up to the last step with the exception that the SS sets the expiration time to 10 seconds in Step 1 of Expected Sequence.

2) After completing the IMS emergency registration UE starts the process of initiating an emergency call, by executing the generic test procedure in steps 1-3 of Annex C.22.

2A-2D) The UE re-registers for IMS emergency services.

3) The SS accepts the call.

4) The UE acknowledges call acceptance.

5) The UE is made to release the call.

6) The SS answers the call release.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Steps defined in annex C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. SS sets the expiration time of emergency registration to 10 seconds.
2			Steps 1-3 defined in annex C.22.	IMS emergency call setup with PSAP using preconditions
2A	→		REGISTER	UE re-registers to the emergency services in a time span between half of the expiration time and the full expiration time. Note: in this test case, the re-registration time is set to an untypically short value of 10 seconds. As there are no requirements on the duration of a re-registration procedure it is only checked that the re-registration procedure starts between half of the expiration time and the full expiration time.
2B	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
2C	→		REGISTER	UE completes the security negotiation procedures, sets up a new temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
2D	←		200 OK	The SS responds with 200 OK.
3	←		200 OK	Response for INVITE sent in step 2 Note: 200 OK will be sent using previous socket connection before using old SA
4	→		ACK	Response from UE to confirm the dialog
5	→		BYE	The UE releases the call with BYE
6	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

REGISTER (Step 2A)

Use the default message “REGISTER” in annex A.1.1. with condition A2 "Subsequent REGISTER sent over security associations” and the following exceptions applying:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and protected server port of UE. The SIP URI shall contain the *sos* URI parameter.
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous REGISTER

401 Unauthorized for REGISTER (Step 2B)

Use the default message "401 Unauthorized for REGISTER" in annex A.1.2 with the following exceptions:

Header/param	Value/remark
Security-Server	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous Security-Server headers
WWW-Authenticate	
nonce	Base 64 encoding of a new RAND and AUTN

REGISTER (Step 2C)

Use the default message "REGISTER" in annex A.1.1 like in step 1 above. The only difference is that the response value within Authorization header shall have been recalculated based on the nonce received from SS within 401 response.

200 OK for REGISTER (Step 2D)

Use the default message "200 OK for REGISTER" in annex A.1.3 with condition A3 "Response for an emergency registration" and the expires parameter of Contact header set to 1200.

19.5.7.5 Test requirements

All the messages specified for this test case shall be sent over the EPS emergency bearers allocated for the initial emergency registration.

19.5.8 Void

19.5.9 In parallel emergency and non-emergency registrations

19.5.9.1 Definition

Test to verify that the UE handles the IMS emergency registration and related signalling independently from any other ongoing IMS registration.

19.5.9.2 Conformance requirement

[TS 24.229 clause 5.1.6.2]:

When the UE performs an initial emergency registration and whilst this emergency registration is active, the UE shall:

- handle the emergency registration independently from any other ongoing registration to the IM CN subsystem;
- handle any signalling or media related IP-CAN for the purpose of emergency calls independently from any other established IP-CAN for IM CN subsystem related signalling or media; and
- handle all SIP signalling and all media related to the emergency call independently from any other ongoing IM CN subsystem signalling and media.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.6.2 (release 9)

19.5.9.3 Test purpose

1) To verify that the UE maintains the emergency call even if the network would initiate the deregistration procedure for the non-emergency IMS registration

19.5.9.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call

16) SS sends a SIP NOTIFY request in order to terminate the non-emergency IMS registration.

17) UE responds the NOTIFY request with 200 OK response. The emergency call remains unaffected on the UE.

18) Emergency call is terminated manually on the UE. Consequently the UE sends SIP BYE request.

19) SS responds the BYE request with 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
16	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing partial registration state information, with all previously registered non-emergency public user identities as "terminated" and "rejected"
17	→		200 OK	The UE responds the NOTIFY with 200 OK
18	→		BYE	The UE releases the emergency call with BYE
19	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

NOTIFY (Step 16)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with the following exceptions:

Header/param	Value/remark
CSeq Value	 2
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<reginfo xmlns="urn:ietf:params:xml:ns:reginfo" version="1" state="partial">* *<registration aor=*"PublicUserIdentity2 (NOTE 1)" *id="a102" state="terminated">* *<contact id="980" state="terminated" event="rejected">* *<uri>*same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>* *<registration aor=*"AssociatedTelUri(NOTE 1)" *id="a101" state="terminated">* *<contact id="981" state="terminated" event="rejected">* *<uri>*same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>* *</reginfo>*

NOTE 1: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI;
AssociatedTelUri is the same as used in P-Associated-URI
PublicUserId2 and PublicUserId3 are the remaining IMPUs of the P-Associated-URI header

200 OK for NOTIFY (Step 17)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

BYE (Step 18)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 19)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

19.5.9.5 Test requirements

UE maintains the IMS emergency call even if the non-emergency IMS registration is terminated by the SS.

19.5.10 Deregistration upon emergency registration expiration

19.5.10.1 Definition

Test to verify that when there is no emergency call going on or being set up, neither there are any standalone transactions related to the IMS emergency registration when half of the time for IMS emergency registration has expired, the UE will not extend the IMS emergency registration but instead silently wait for the emergency registration to expire.

19.5.10.2 Conformance requirement

[TS 24.229 clause 5.1.6.4]:

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if half of the time for the emergency registration has expired and:

- the UE has emergency related ongoing dialog; or
- standalone transactions exist; or
- the user initiates an emergency call.

The UE shall not perform user-initiated emergency reregistration in any other cases.

[TS 24.229 clause 5.1.6.6]:

Once the UE registers a public user identity and an associated contact address via emergency registration, the UE shall not perform user-initiated deregistration of the respective public user identity and the associated contact address.

NOTE: The UE will be deregistered when the emergency registration expires.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.4 and 5.1.6.6

19.5.10.3 Test purpose

1) To verify that the UE will not reregister to IMS emergency services in the absence of emergency related dialog, standalone transaction and emergency call initiation.

19.5.10.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call. As an exception the SS sets the expiration time to 100 seconds in Step 4 of Annex C.20.

16) Void.

17) Void.

18-22) The emergency call is terminated on the UE 20 seconds after it has been initiated. Steps defined in annex C.32 are followed.

23-24) Emergency Bearer context is deactivated.

25) The UE does not send any message before the IMS Emergency Reregistration time has elapsed.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
16				Void.
17				Void.
18-22			Steps defined in clause C.32	The emergency call is terminated on the UE 20 seconds after it has been initiated.
23-24			EPS emergency bearer context deactivation by the SS.	EPS Bearer Deactivation procedure according TS 36.508 [94] clause 4.5A.15, applied to the identity of the Default EPS Bearer of the emergency PDN.
25				The SS waits for the IMS Emergency Reregistration time elapse

19.5.10.5 Test requirements

The UE shall not send IMS emergency reregistration within the expiration time specified in step 1.

20 Customized Alerting Tones (CAT)

20.1 Mobile Originating CAT – Forking Model

20.1.1 Definition

Test to verify that the UE support Customized Alerting Tones according to the forking model. This process is described in 3GPP TS 24.182 [127].

20.1.2 Conformance requirement

[TS 24.182, clause 4.5.5.1.1]:

The UE shall follow the procedures specified in 3GPP TS 24.229 for session initiation and termination.

[TS 24.628, clause 4.7.2.1]:

Procedures according to 3GPP TS 24.229 shall apply.

Certain services require the usage of the Alert-Info header field, Call-Info header field and Error-Info header field according to procedures specified by IETF RFC 3261.

If the UE detects that in-band information is received from the network as early media, the in-band information received from the network shall override locally generated communication progress information.

The UE shall not generate the locally generated communication progress information if an early dialog exists where the last received P-Early-Media header field as described in IETF RFC 5009 contains "sendrecv" or "sendonly".

NOTE: if an early dialog exists where a SIP 18x response to the SIP INVITE request other than 183 (Session Progress) response was received, no early dialog exists where the last received P-Early-Media header field as described in IETF RFC 5009 contained "sendrecv" or "sendonly" and in-band information is not received from the network, then the UE is expected to render the locally generated communication progress information.

If the UE supports the P-Early-Media header field as defined in IETF RFC 5009, and a P-Early-Media header field has been received, then the UE shall send any available user generated media, e.g. speech or DTMF, on media stream(s) associated with the early dialog for which the most recent P-Early-Media header field, as described in IETF RFC 5009, contained a "sendrecv" or a "recvonly" header field value. If there is more than one such early dialog, the UE shall use the early dialog where the P-Early-Media header field was most recently received.

If the UE receives a re-INVITE request containing no SDP offer, the UE shall send a 200 (OK) response containing an SDP offer according to 3GPP TS 24.229 indicating the directionality used by UE as

- "sendonly" if the re-INVITE request is received on a dialog where the associated communication session has been put on hold by the user; and
- "sendrecv" otherwise.

Reference(s)

3GPP TS 24.182 [127], clause 4.5.5.1.1 and 3GPP TS 24.628 [128], clause 4.7.2.1.

20.1.3 Test purpose

1) To verify that when initiating MO call, with Customized Alerting Tones according to the forking model, the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and
2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating early media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1).

20.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, and registered to IMS services.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-13) UE executes the procedures described in TS 36.508 [94] table 4.5A.21.3-1 steps 1 to14.

14) SS responds to the INVITE sent by the UE in step 2 with a 200 OK to create dialog 1.

15) UE sends ACK to acknowledge receipt of the 200 OK for INVITE.

16) UE is triggered by MMI to release the call

17) UE sends a BYE request to the SS in order to release the call.

18) SS responds to the BYE request with a valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Perform steps 1 to 8 of the procedure detailed in C.21	Setup dialog 1
9-13			Perform steps 4 to 8 of the procedure detailed in C.21	Setup dialog 2 (CAT)
14	←		200 OK	The SS sends 200 OK for INVITE sent in step 2 above (dialog 1)
15	→		ACK	The UE sends ACK for the 200 OK
16			The UE is triggered by MMI to release the call	
17	→		BYE	The UE releases the call with BYE
18	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition “IMS security” or “GIBA” when applicable

Specific Message Contents

Steps 1 – 8 and 9-13 as specified in annex C.21 with the exceptions detailed below

INVITE (Step 2)

Use the default message “INVITE” in step 2 of annex C.21

183 Session Progress (Step 9)

Use the default message "183 Session Progress" in step 4 of annex C.21 with the following exceptions:

Header/param	Value/Remark
To tag	 Any value different from what is used in steps 1-8
Contact addr-spec	 *<sip:cat-as.home1.net;+g.3gpp.icsi_ref="urn%3Aurn-7%3gpp-service.ims.icsi.mmtel">*
P-Early-Media em-param	 *sendonly*
Message-body	Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS for early-media) - *s=-* - *c=IN* (addrtype) (connection-address for SS for early-media) - *b=AS:37* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Other attributes: - *a=content:g.3gpp.cat*

PRACK (Step 10)

Use the default message “PRACK” in step 5 of annex C.21 with the following exceptions:

Header/param	Value/Remark
Message-body	Header optional Contents if present is copied from step 5 of annex C.21 with the following exceptions: Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv*

200 OK for PRACK (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
To tag	 Same value as used in step 9
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if PRACK in step 10 contained a SDP. Contents if present: SDP body of the 200 OK response copied from the received PRACK and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media (same as used in step 9 above); - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

200 OK for UPDATE (Step 13)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
To tag	 Same value as used in step 9
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media (same as used in step 9 above); - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

200 OK (Step 14)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 OK response copied from the received PRACK and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

BYE (Step 17)

Use the default message "BYE" in annex A.2.8.

200 OK for BYE (Step 18)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

20.1.5 Test requirements

SS must check that the if the UE uses full IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

The UE shall send requests and responses as described in clause 20.1.4.

21 eCall over IMS

For the eCall over IMS test cases, the default USIM settings are specified in TS 36.508 [94] clause 4.9.3.5.

21.1 eCall over IMS / Manual initiation / Normal registration / Emergency registration / Success / 200 OK with ACK

21.1.1 Definition

Test to verify that the UE can correctly perform eCall over IMS when initiated manually and that the SS releases the call after 200 OK with ACK is received. The process consists of emergency registration and MSD included in INVITE during call setup.

21.1.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.1]:

If the upper layers request establishment of an IMS emergency call of the manually initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.manual" as specified in RFC 8147 [244].

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.automatic" as specified in RFC 8147 [244].

NOTE: The manually initiated eCall type of emergency service is used when the eCall IMS emergency session is invoked with user input. The automatically initiated eCall type of emergency service is used if the eCall IMS emergency session is invoked without user input.

[TS 24.229, clause 5.1.6.11.2]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

   a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

   b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

   c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

…

2) if the UE receives a 200 (OK) response to the INVITE request containing:

   a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

i) a "received" attribute set to "true"; and

ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

then the UE shall consider the initial MSD transmission as successful;

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.11.1 and 5.1.6.11.2.

21.1.3 Test purpose

1) To verify that the UE can correctly register to IMS emergency services and initiate an eCall over IMS in manual mode when UE is registered to IMS non-emergency services, according to TS 24.229 [10] clause 5.1.6.11.1;

2) To verify that the UE sends a correctly composed initial INVITE request for eCall over IMS and will complete the eCall session setup after receiving 200 OK with ACK, according to 3GPP TS 24.229 [10] clause 5.1.6.11.2.

21.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application with eCall subscription on UICC. The UE has discovered P-CSCF, and registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Manual eCall over IMS initiated at UE

2) Emergency registration according to C.20 is executed

3) SS waits for UE to send an INVITE request.

4) SS sends 200 OK with ACK.

5) Void

6)-9) MT Call release according to steps 1-4 of procedure C.33.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			UE is triggered to initiate a manual eCall	
2-5			Steps 1-4 defined in C.20	IMS emergency registration. Referred from 36.508 [94] table 4.5A.26.3-1 for a UE with E-UTRA support.
6-8			Steps 1-3 defined in C.47	eCall setup
9-12			Steps 1-4 defined in C.33	The SS releases the call

Specific Message Contents

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A20.

Step 7 as specified in annex C.47, which is referring to A.3.1 default message content of 200 OK with condition A13.

BYE (Step 9)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 10)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

21.1.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for manual eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

21.2 eCall over IMS / Automatic initiation / Normal registration / Emergency registration / Success / 200 OK with ACK

21.2.1 Definition

Test to verify that the UE can correctly perform eCall over IMS when initiated automatically and that the SS releases the call after 200 OK with ACK is received. The process consists of emergency registration and MSD included in INVITE during call setup.

21.2.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.1]:

If the upper layers request establishment of an IMS emergency call of the manually initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.manual" as specified in RFC 8147 [244].

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.automatic" as specified in RFC 8147 [244].

NOTE: The manually initiated eCall type of emergency service is used when the eCall IMS emergency session is invoked with user input. The automatically initiated eCall type of emergency service is used if the eCall IMS emergency session is invoked without user input.

[TS 24.229, clause 5.1.6.11.2]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

   a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

   b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

   c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

…

2) if the UE receives a 200 (OK) response to the INVITE request containing:

   a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

      i) a "received" attribute set to "true"; and

      ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

   then the UE shall consider the initial MSD transmission as successful;

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.11.1 and 5.1.6.11.2.

21.2.3 Test purpose

1) To verify that the UE can correctly register to IMS emergency services and initiate an eCall over IMS in automatic mode when UE is registered to IMS non-emergency services, according to TS 24.229 [10] clause 5.1.6.11.1;

2) To verify that the UE sends a correctly composed initial INVITE request for eCall over IMS and will complete the eCall session setup after receiving 200 OK with ACK, according to 3GPP TS 24.229 [10] clause 5.1.6.11.2.

21.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall subscription. The UE has discovered P-CSCF, and registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Automatic eCall over IMS initiated at UE

2) Emergency registration according to C.20 is executed

3) SS waits for UE to send an INVITE request.

4) SS sends 200 OK with ACK.

5) Void

6)-9) MT Call release according to steps 1-4 of procedure C.33.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			UE is triggered to initiate an automatic eCall	
2-5			Steps 1-4 defined in C.20	IMS emergency registration. Referred from 36.508 [94] table 4.5A.26.3-1 for a UE with E-UTRA support.
6-8			Steps 1-3 defined in C.47	eCall setup
9-12			Steps 1-4 defined in C.33	The SS releases the call

Specific Message Contents

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A21.

Step 7 as specified in annex C.47, which is referring to A.3.1 default message content of 200 OK with condition A13.

BYE (Step 9)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 10)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

21.2.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for automatic eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

21.3 eCall over IMS / Manual initiation / MSD transfer Failure / UE performs eCall in CS domain after Timer expiry / UTRAN or GERAN

21.3.1 Definition

Test to verify that the UE performs eCall in CS domain after MSD transfer failed during manual eCall Initiation. This process is described in 3GPP TS 24.229 [10].

21.3.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.3]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

   a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

1) if the UE receives a 200 (OK) response to the INVITE request not containing:

a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

i) a "received" attribute set to "true"; and

ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

then the UE shall send the MSD using audio media stream encoded as described in 3GPP TS 26.267 [9C];

2) if the UE receives a 200 (OK) response to the INVITE request containing:

a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

i) a "received" attribute set to "true"; and

ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

then the UE shall consider the initial MSD transmission as successful;

3) if the UE receives a 486 (Busy Here), 600 (Busy Everywhere) or 603 (Decline) response to the INVITE request containing:

a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

i) a "received" attribute set to "true"; and

ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

then the UE shall consider the initial MSD transmission as successful and shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B]; and

4) in all other cases, the UE shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B].

Reference(s)

3GPP TS 24.229 [10], clause 5.1.6.11.2.

21.3.3 Test purpose

1) To verify that when the UE transmits eCall MSD with SIP INVITE, it waits for timer expiry to receive 200OK from network according to 3GPP TS 24.229 [10] 5.1.6.11.1 and 5.1.6.11.2

2) To verify that the UE make eCall over CS domain after timer expiry

21.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall subscription. UE has discovered P-CSCF, and registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell A power level is set as “serving cell” and cell 24/cell 5 power level is set as “suitable cell”

Note: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Manual eCall initiated at UE.2-5) Executes the procedures described in TS 36.508 [94] table 4.5A.26.3-1 steps 2 to 15 and parallel behaviour steps 1-4 for EPS emergency bearer context activation, and subsequent IMS emergency registration

6) SS waits for UE to send an INVITE request.

7) SS waits until expiry of emerg-request timer(15 seconds) so that transfer of MSD transfer fails

8-9) UE performs domain selection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM registration if necessary. CS eCall is established. CS eCall is maintained for at least 5 seconds and then the call is cleared by SS.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt manual eCall Call	
2-5			Step 1-4 defined in C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. Referred from 36.508 [94] table 4.5A.26.3-1 for a UE with E-UTRA support.
6			Step1 defined in C.47	UE sends INVITE along with initial SDP offer and MSD
7				SS waits until expiry of emerg-request timer(15 seconds) so that transfer of MSD fails
			EXCEPTION: The UE performs a domain selection for the emergency call and within 2 seconds after step 7 the UE may transmit EXTENDED SERVICE REQUEST	
8a1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8a2			SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
			EXCEPTION: Either step 9a1 or 9b1 is performed, depending on the value of px_RATComb_Tested	
9a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs CS fallback or cell reselection to a cell supporting CS domain (UTRAN) and performs eCall establishment in CS domain together with MM/GMM registration	NOTE 3: RAU procedure can take place in parallel to emergency CS call.
9a2			eCall is maintained for at least 5 seconds	
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration defined in Annex C.46 of TS 34.229-1 can take place	
9a3			SS configures cell A as a “non-suitable cell”	
9a4			eCall is cleared by SS	
9b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs CS fallback or cell reselection to a cell supporting CS domain (GERAN cell) and performs eCall establishment in CS domain	
9b2			eCall is maintained for at least 5 seconds	
9b3			SS configures cell A as a “non-suitable cell”	
9b4			eCall is cleared by SS	
9b5			UE performs MM/GMM registration	

Specific Message Contents

Step 2 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A20.

RRCConnectionRelease (step 8a2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (Step 9b5)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

21.3.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for manual eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

In step 9a1 or 9b1, UE shall send an EMERGENCY SETUP message with the Service Category IE bit 6 = 1 and all other bits are set to 0.

21.4 eCall over IMS / Manual initiation / MSD transfer and 200 OK with ACK / SIP INFO request for MSD Update / Success

21.4.1 Definition

Test to verify that the UE retry MSD transfer after MSD transfer failed during manual eCall Initiation. This process is described in 3GPP TS 24.229 [10].

21.4.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.3]:

During an emergency session established for eCall type of emergency service as described in subclause 5.1.6.11.2, if the UE receives an INFO request with:

1) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

2) a multipart/mixed body including:

a) an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] containing a "request" element with an "action" attribute set to "send-data" and a "datatype" attribute set to "eCall.MSD"; and

b) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.Control+xml" MIME body part; and

3) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body;

the UE shall proceed as follows:

1) if the UE is able to provide an updated MSD, the UE shall send an INFO request containing:

a) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

b) a multipart/mixed body including:

i) an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244] containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 as specified in CEN EN 15722:2015 [245]; and

ii) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.eCall.MSD" MIME body part; and

c) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body; and

2) if the UE is not able to provide an updated MSD, the UE shall send an INFO request containing:

a) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

b) a multipart/mixed body including:

i) an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

- a "ref" attribute set to the Content-ID of the "application/EmergencyCallData.Control+xml" MIME body part in the INFO request received by the UE; and

- an "actionResult" child element containing:

A) an "action" attribute set to "send-data";

B) a "success" attribute set to "false"; and

C) a "reason" attribute set to an appropriate value as defined in RFC 8147 [244]; and

ii) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.Control+xml" MIME body part; and

c) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body.

NOTE: Further content for the INFO request is as defined in RFC 8147 [244].

Reference(s)

3GPP TS 24.229 [10], clause 5.1.6.11.2.

21.4.3 Test purpose

1) To verify that the UE transmits eCall MSD with SIP INVITE for eCall over IMS in manual mode and receives corresponding 200 OK with ACK.

2) To verify that PSAP uses a SIP INFO with correct FROM-header to request an updated MSD and UE ACK the SIP INFO with a 200 OK.

3) UE sends updated MSD in a SIP INFO with correct Request-URI and To-header. PSAP ACK the updated MSD with 200 OK.

21.4.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall subscription. UE has discovered P-CSCF, and registered to IMS services.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Manual eCall initiated at UE.
2) Emergency registration according to C.20 is executed
3) SS waits for UE to send an INVITE request.
4) SS sends with 200 OK.
5) SS waits for ACK.
6) SS sends INFO request to transfer MSD.
7) SS expects and receives 200 OK.
8) SS expects and receives INFO request from the UE with MSD contents.
9) SS responds with 200 OK for INFO request from UE.
10) SS sends BYE to the UE.
11) SS expects and receives 200 OK for BYE from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt manual eCall	
2-5			Steps 1-4 defined in C.20	IMS emergency registration. Referred from 36.508 [94] table 4.5A.26.3-1 for a UE with E-UTRA support.
6-12			Steps 1-7 defined in C.47	eCall setup
13	←		BYE	The SS sends BYE to release the call.
14	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

Specific Message Contents:

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A20.

Step 7 as specified in annex C.47, which is referring to A.3.1 default message content of 200 OK with condition A13.

21.4.5 Test requirements

The UE shall send requests and responses as described in clause 21.4.4.

21.5 eCall over IMS / Automatic initiation / MSD transfer and 200 OK with ACK / SIP INFO request for MSD Update / Success

21.5.1 Definition

Test to verify that the UE updates MSD successfully after automatic eCall established using SIP INFO procedure. This process is described in 3GPP TS 24.229 [10].

21.5.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.3]:

During an emergency session established for eCall type of emergency service as described in subclause 5.1.6.11.2, if the UE receives an INFO request with:

1) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

2) a multipart/mixed body including:

    a) an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] containing a "request" element with an "action" attribute set to "send-data" and a "datatype" attribute set to "eCall.MSD"; and

    b) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.Control+xml" MIME body part; and

3) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body;

the UE shall proceed as follows:

1) if the UE is able to provide an updated MSD, the UE shall send an INFO request containing:

    a) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

    b) a multipart/mixed body including:

        i) an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244] containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 as specified in CEN EN 15722:2015 [245]; and

        ii) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.eCall.MSD" MIME body part; and

    c) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body; and

2) if the UE is not able to provide an updated MSD, the UE shall send an INFO request containing:

    a) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

    b) a multipart/mixed body including:

        i) an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

            - a "ref" attribute set to the Content-ID of the "application/EmergencyCallData.Control+xml" MIME body part in the INFO request received by the UE; and

            - an "actionResult" child element containing:

                A) an "action" attribute set to "send-data";

                B) a "success" attribute set to "false"; and

C) a "reason" attribute set to an appropriate value as defined in RFC 8147 [244]; and

ii) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.Control+xml" MIME body part; and

c) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body.

NOTE: Further content for the INFO request is as defined in RFC 8147 [244].

Reference(s)

3GPP TS 24.229 [10], clause 5.1.6.11.2

21.5.3 Test Purpose

1) To verify that the UE transmits eCall MSD with SIP INVITE for eCall over IMS in automatic mode and receives 200 OK with ACK.

2) To verify that PSAP uses a SIP INFO with correct FROM-Header to request an updated MSD and UE ACK the SIP INFO with a 200 OK.

3) UE sends updated MSD in a SIP INFO with correct Request-URI and To-header. PSAP ACK the updated MSD with 200 OK.

21.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall subscription. UE has discovered P-CSCF, and registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Automatic eCall over IMS initiated at UE

2-5) UE executes the procedures described in TS 36.508 [94] table 4.5A.26.3-1 steps 2 to 15 and parallel behaviour steps 1-4 for EPS emergency bearer context activation, and subsequent IMS emergency registration,

6-12) eCall is established successfully and MSD transferred successfully using INFO procedure as defined in C.47

13) SS sends BYE to the UE

14) SS expects and receives 200 OK for BYE from the UE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE to initiate automatic eCall	
2-5			Steps 1-4 defined in C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. Referred from 36.508 [94] table 4.5A.26.3-1 for a UE with E-UTRA support.
6-12			Steps 1-7 defined in C.47	eCall Setup and MSD transfer using INFO message
13	←		BYE	The SS sends BYE to release the call.
14	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

Specific Message Contents:

Step 1 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A21.

Step 2 as specified in annex C.47, which is referring to A.3.1 default message content of 200 OK with condition A12 and A13.

21.5.5 Test requirements

UE shall update MSD as defined in steps 11-12.

21.6 eCall over IMS / Automatic initiation / MSD transfer and 200 OK with ACK / SIP INFO request for unsupported MSD / UE indicates unsuccessful in SIP INFO

21.6.1 Definition

Test to verify that the UE sends SIP INFO with correct contents as a response to SIP INFO with unsupported MSD transfer upon automatic eCall Initiation. This process is described in 3GPP TS 24.229 [10].

21.6.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.3]:

During an emergency session established for eCall type of emergency service as described in subclause 5.1.6.11.2, if the UE receives an INFO request with:

1) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

2) a multipart/mixed body including:

   a) an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] containing a "request" element with an "action" attribute set to "send-data" and a "datatype" attribute set to "eCall.MSD"; and

   b) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.Control+xml" MIME body part; and

3) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body;

the UE shall proceed as follows:

1) if the UE is able to provide an updated MSD, the UE shall send an INFO request containing:

   a) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

b) a multipart/mixed body including:

i) an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244] containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 as specified in CEN EN 15722:2015 [245]; and

ii) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.eCall.MSD" MIME body part; and

c) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body; and

2) if the UE is not able to provide an updated MSD, the UE shall send an INFO request containing:

a) an Info-Package header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244];

b) a multipart/mixed body including:

i) an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

- a "ref" attribute set to the Content-ID of the "application/EmergencyCallData.Control+xml" MIME body part in the INFO request received by the UE; and

- an "actionResult" child element containing:

A) an "action" attribute set to "send-data";

B) a "success" attribute set to "false"; and

C) a "reason" attribute set to an appropriate value as defined in RFC 8147 [244]; and

ii) a Content-Disposition header field set to "By-Reference" associated with the "application/EmergencyCallData.Control+xml" MIME body part; and

c) a Content-Disposition header field set to "Info-Package" associated with the multipart/mixed body.

NOTE: Further content for the INFO request is as defined in RFC 8147 [244].

Reference(s)

3GPP TS 24.229 [10], clause 5.1.6.11.2

21.6.3 Test purpose

1) To verify that the UE transmits eCall MSD with SIP INVITE for eCall over IMS in automatic mode and receives 200 OK with ACK.

2) To verify that PSAP uses a SIP INFO with correct FROM-Header to request an unsupported MSD and UE ACK the SIP INFO with a 200 OK.

3) UE responds with SIP INFO with correct contents with indication of unsuccessful transfer. PSAP returns 200 OK.

21.6.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall subscription. UE has discovered P-CSCF, and registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Automatic eCall over IMS initiated at UE

2-5) UE executes the procedures described in TS 36.508 [94] table 4.5A.26.3-1 steps 2 to 15 and parallel behaviour steps 1-4 for EPS emergency bearer context activation, and subsequent IMS emergency registration,

6-7) eCall is established successfully

8-11) Execute MSD transfer procedure as defined in Annex C.47 from steps 4-7

12) SS sends BYE to the UE

13) SS expects and receives 200 OK for BYE from the UE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt Automatic eCall	
2-5			Step 1-4 defined in C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. Referred from 36.508 [94] table 4.5A.26.3-1 for a UE with E-UTRA support.
6-7			Steps 1-3 defined in C.47	eCall over IMS initiated automatically. Referred from 36.508 [94] table 4.5A.26.3-1 for a UE with E-UTRA support.
8-11			Steps 4-7 defined in C.47	eCall over IMS initiated automatically. Referred from 36.508 [94] table 4.5A.26 for a UE with E-UTRA support.
12	←		BYE	The SS sends BYE to release the call.
13	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable

Specific Message Contents:

Step 1 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A21.

Step 2 as specified in annex C.47, which is referring to A.3.1 default message content of 200 OK with condition A12 and A13.

Step 8 as specified in Annex C.47 except datatype attribute with the value ‘eCall.invalidMSD’ in message body

Step 10 as specified in annex C.47, which is referring to A.2.19 default message content of MO INFO with condition A4.

21.6.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for automatic eCall over IMS.

In step 10, UE shall transmit MO INFO with ‘success’ attribute set to “false” in message body.

21.7 to 21.12 Void

21.13 eCall only mode / Manual initiation / Emergency registration / Abnormal case / IM CN sends a 486 (Busy Here) / UE performs eCall in CS domain / UTRAN or GERAN

21.13.1 Definition

Test to verify that on reception of reject cause 486 Busy here for a manually initiated INVITE for eCall over IMS, UE initiates the eCall in supported CS domain over UTRAN or GERAN.

21.13.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.1]:

If the upper layers request establishment of an IMS emergency call of the manually initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.manual" as specified in RFC 8147 [244].

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.automatic" as specified in RFC 8147 [244].

NOTE: The manually initiated eCall type of emergency service is used when the eCall IMS emergency session is invoked with user input. The automatically initiated eCall type of emergency service is used if the eCall IMS emergency session is invoked without user input.

[TS 24.229, clause 5.1.6.11.2]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

   a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

   b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

   c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

…

3) if the UE receives a 486 (Busy Here), 600 (Busy Everywhere) or 603 (Decline) response to the INVITE request containing:

   a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

      i) a "received" attribute set to "true"; and

      ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

then the UE shall consider the initial MSD transmission as successful and shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B]; and

4) in all other cases, the UE shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B].

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.11.1 and 5.1.6.11.2.

21.13.3 Test purpose

1) To verify that the UE is able to handle 486 (Busy here) SIP error message for a manually initiated INVITE for eCall over IMS; and

2) To verify that the UE is able to establish legacy eCall in CS domain in UTRAN or GERAN system after receiving 486 (Busy here) SIP error message.

21.13.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall Only subscription. UE is switched on not registered to IMS services.

The SS is configured:

- with 2 cells: as in TS 36.508 [94]
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell A power level is set as "serving cell" and cell 24/cell 5 power level is set as "suitable cell"

NOTE: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Manual eCall over IMS initiated at UE

1A-1H) IMS registration according to C.2 is executed.

2-5) IMS Emergency registration according to C.20 is executed.

6) SS waits for UE to send an INVITE request.

7) SS sends 486 Busy here.

8-9) UE performs domain selection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM registration if necessary. CS eCall is established and maintained for 5 seconds and then the call is cleared by SS.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			UE is triggered to initiate a manual eCall	Step 2 in generic procedure 36.508 [94] table 4.5A.27.3-1.
2-5			Steps 1-4 defined in Annex C.20	Steps 19 to 25 in generic procedure 36.508 [94] table 4.5A.27.3-1. UE establishes the emergency PDN and performs IMS emergency registration.
6			Step 1 defined in C.47	eCall setup is initiated.
7	←		486 Busy here	The SS sends 486 Busy here
			EXCEPTION: The UE performs a domain selection for the emergency call and within 2 seconds of step 7 the UE may transmit EXTENDED SERVICE REQUEST	
8a1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8a2			SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
			EXCEPTION: Either step 9a1 or 9b1 is performed, depending on the value of px_RATComb_Tested	
9a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs domain selection to a cell supporting CS domain (UTRAN) and performs eCall establishment in CS domain together with MM registration	NOTE: RAU procedure can take place in parallel to normal CS call.
9a2			SS configures cell A as a “non-suitable cell”	
9a3			eCall is maintained for 5 seconds	
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration defined in Annex C.46 of TS 34.229-1 can take place	
9a4			eCall is cleared by SS	
9b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs domain selection to a cell supporting CS domain (GERAN cell) and performs eCall establishment in CS domain	
9b2			SS configures cell A as a “non-suitable cell”	
9b3			eCall is maintained for 5 seconds	
9b4			eCall is cleared by SS	
9b5			UE performs MM/GMM registration	

Specific Message Contents

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A20
Step 7 486 Busy Here message as in Annex A.2.21

RRCConnectionRelease (step 8a2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (Step 9b5)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

21.13.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for manual eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

In step 9a1 or 9b1, UE shall send an EMERGENCY SETUP message with the Service Category IE bit 6 = 1 and all other bits are set to 0.

21.14 eCall only mode / Automatic initiation / Emergency registration / Abnormal case / IM CN sends a 486 (Busy Here) / UE performs eCall in CS domain / UTRAN or GERAN

21.14.1 Definition

Test to verify that on reception of reject cause 486 Busy here for automatically initiated INVITE for eCall over IMS, UE initiates the eCall in supported CS domain over UTRAN or GERAN.

21.14.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.1]:

If the upper layers request establishment of an IMS emergency call of the manually initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.manual" as specified in RFC 8147 [244].

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.automatic" as specified in RFC 8147 [244].

NOTE: The manually initiated eCall type of emergency service is used when the eCall IMS emergency session is invoked with user input. The automatically initiated eCall type of emergency service is used if the eCall IMS emergency session is invoked without user input.

[TS 24.229, clause 5.1.6.11.2]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

   a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

   b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

   c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

…

3) if the UE receives a 486 (Busy Here), 600 (Busy Everywhere) or 603 (Decline) response to the INVITE request containing:

   a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

      i) a "received" attribute set to "true"; and

      ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

   then the UE shall consider the initial MSD transmission as successful and shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B]; and

4) in all other cases, the UE shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B].

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.11.1 and 5.1.6.11.2.

21.14.3 Test purpose

1) To verify that the UE is able to handle 486 (Busy here) SIP error message for an Automatically initiated INVITE for eCall over IMS; and

2) To verify that the UE is able to establish legacy eCall in CS domain in UTRAN or GERAN system after receiving 486 (Busy here) SIP error message.

21.14.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall Only subscription. The UE is switched on not registered to IMS services.

The SS is configured:

- with 2 cells: as in TS 36.508 [94]
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell A power level is set as “serving cell” and cell 24/cell 5 power level is set as “suitable cell”

NOTE: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Automatic eCall over IMS is initiated at the UE

1A-1H) IMS registration according to C.2 is executed.

2-5) Emergency registration according to C.20 is executed.

6) SS waits for UE to send an INVITE request

7) SS sends 486 Busy here.

8-9) UE performs domain selection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM registration if necessary. CS eCall is established and maintained for 5 seconds and then the call is cleared by SS.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			UE is triggered to initiate an automatic eCall	Step 2 in generic procedure 36.508 [94] table 4.5A.27.3-1.
1A-1H			Steps 4-11 in Annex C.2	Steps 3 to 18 in generic procedure in 36.508 [94] table 4.5A.27.3-1. UE attaches to the NW, establishes the default PDN, and performs IMS registration.
2-5			Step 1-4 defined in C.20	Steps 19 to 25 in generic procedure 36.508 [94] table 4.5A.27.3-1. UE establishes the emergency PDN and performs IMS emergency registration.
6			Step1 defined in C.47	UE sends INVITE along with initial SDP offer and MSD
7	←		486 Busy here	The SS sends 486 Busy here
			EXCEPTION: The UE performs a domain selection for the emergency call and the UE may transmit EXTENDED SERVICE REQUEST	
8a1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8a2			SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
			EXCEPTION: Either step 9a1 or 9b1 is performed, depending on the value of px_RATComb_Tested	
9a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs domain selection to a cell supporting CS domain (UTRAN) and performs eCall establishment in CS domain together with MM registration	NOTE: RAU procedure can take place in parallel to normal CS call.
9a2			SS configures cell A as a “non-suitable cell”	
9a3			eCall is maintained for 5 seconds	
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration defined in Annex C.46 of TS 34.229-1 can take place	
9a4			eCall is cleared by SS	
9b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs domain selection to a cell supporting CS domain (GERAN cell) and performs eCall establishment in CS domain	
9b2			SS configures cell A as a “non-suitable cell”	
9b3			eCall is maintained for 5 seconds	
9b4			eCall is cleared by SS	
9b5			UE performs MM/GMM registration	

Specific Message Contents

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A21
Step 7 486 Busy Here message as in Annex A.2.21.

RRCConnectionRelease (step 8a2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (Step 9b5)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

21.14.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for Automatic eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

In step 9a1 or 9b1, UE shall send an EMERGENCY SETUP message with the Service Category IE bit 7= 1 and all other bits are set to 0.

21.15 eCall only mode / Manual initiation / Emergency registration / Abnormal case / IM CN sends a 600 (Busy Everywhere) / UE performs eCall in CS domain / UTRAN or GERAN

21.15.1 Definition

Test to verify that on reception of reject cause 600 Busy everywhere for a manually initiated INVITE for eCall over IMS, UE initiates the eCall in supported CS domain over UTRAN or GERAN.

21.15.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.1]:

If the upper layers request establishment of an IMS emergency call of the manually initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.manual" as specified in RFC 8147 [244].

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.automatic" as specified in RFC 8147 [244].

NOTE: The manually initiated eCall type of emergency service is used when the eCall IMS emergency session is invoked with user input. The automatically initiated eCall type of emergency service is used if the eCall IMS emergency session is invoked without user input.

[TS 24.229, clause 5.1.6.11.2]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

   a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

   b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

   c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

…

3) if the UE receives a 486 (Busy Here), 600 (Busy Everywhere) or 603 (Decline) response to the INVITE request containing:

   a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

      i) a "received" attribute set to "true"; and

      ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

   then the UE shall consider the initial MSD transmission as successful and shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B]; and

4) in all other cases, the UE shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B].

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.11.1 and 5.1.6.11.2.

21.15.3 Test purpose

1) To verify that the UE is able to handle 600 (Busy Everywhere) SIP error message for a manually initiated INVITE for eCall over IMS; and

2) To verify that the UE is able to establish legacy eCall in CS domain in UTRAN or GERAN system after receiving 600 (Busy Everywhere) SIP error message.

21.15.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall Only subscription. The UE is switched on not registered to IMS services.

The SS is configured:

- with 2 cells: as in TS 36.508 [94]
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell A power level is set as “serving cell” and cell 24/cell 5 power level is set as “suitable cell”

NOTE: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Manual eCall over IMS is initiated at the UE

1A-1H) IMS registration according to C.2 is executed.

2-5) Emergency registration according to C.20 is executed.

6) SS waits for UE to send an INVITE request

7) SS sends 600 Busy everywhere.

8-9) UE performs domain selection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM registration if necessary. CS eCall is established and maintained for 5 seconds and then the call is cleared by SS.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			UE is triggered to initiate a manual eCall	
1A-1H			Steps 4-11 in Annex C.2	Steps 3 to 18 in generic procedure in 36.508 [94] table 4.5A.27.3-1. UE attaches to the NW, establishes the default PDN, and performs IMS registration.
2-5			Step 1-4 defined in C.20	Steps 19 to 25 in generic procedure 36.508 [94] table 4.5A.27.3-1. UE establishes the emergency PDN and performs IMS emergency registration.
6			Step1 defined in C.47	UE sends INVITE along with initial SDP offer and MSD
7	←		600 Busy everywhere	The SS sends 600 Busy everywhere
			EXCEPTION: The UE performs a domain selection for the emergency call and the UE may transmit EXTENDED SERVICE REQUEST	
8a1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8a2			SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
			EXCEPTION: Either step 9a1 or 9b1 is performed, depending on the value of px_RATComb_Tested	
9a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs domain selection to a cell supporting CS domain (UTRAN) and performs eCall establishment in CS domain together with MM registration	NOTE: RAU procedure can take place in parallel to normal CS call.
9a2			SS configures cell A as a “non-suitable cell”	
9a3			eCall is maintained for 5 seconds	
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration defined in Annex C.46 of TS 34.229-1 can take place	
9a4			eCall is cleared by SS	
9b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs domain selection to a cell supporting CS domain (GERAN cell) and performs eCall establishment in CS domain	
9b2			SS configures cell A as a “non-suitable cell”	
9b3			eCall is maintained for 5 seconds	
9b4			eCall is cleared by SS	
9b5			UE performs MM/GMM registration	

Specific Message Contents

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A20
Step 7 600 Busy Everywhere message as in Annex A.2.22.

RRCConnectionRelease (step 8a2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (Step 9b5)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

21.15.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for manual eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

In step 9a1 or 9b1, UE shall send an EMERGENCY SETUP message with the Service Category IE bit 6 = 1 and all other bits are set to 0.

21.16 eCall only mode / Automatic initiation / Emergency registration / Abnormal case / IM CN sends a 600 (Busy Everywhere) / UE performs eCall in CS domain / UTRAN or GERAN

21.16.1 Definition

Test to verify that on reception of reject cause 600 Busy everywhere for an automatically initiated INVITE for eCall over IMS, UE initiates the eCall in supported CS domain over UTRAN or GERAN.

21.16.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.1]:

If the upper layers request establishment of an IMS emergency call of the manually initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.manual" as specified in RFC 8147 [244].

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.automatic" as specified in RFC 8147 [244].

NOTE: The manually initiated eCall type of emergency service is used when the eCall IMS emergency session is invoked with user input. The automatically initiated eCall type of emergency service is used if the eCall IMS emergency session is invoked without user input.

[TS 24.229, clause 5.1.6.11.2]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

    a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

    b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

    c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

…

3) if the UE receives a 486 (Busy Here), 600 (Busy Everywhere) or 603 (Decline) response to the INVITE request containing:

    a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

        i) a "received" attribute set to "true"; and

        ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

    then the UE shall consider the initial MSD transmission as successful and shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B]; and

4) in all other cases, the UE shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B].

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.11.1 and 5.1.6.11.2.

21.16.3 Test purpose

1) To verify that the UE is able to handle 600 (Busy Everywhere) SIP error message for an automatically initiated INVITE for eCall over IMS; and

2) To verify that the UE is able to establish legacy eCall in CS domain in UTRAN or GERAN system after receiving 600 (Busy Everywhere) SIP error message.

21.16.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall Only subscription. UE is switched on not registered to IMS services.

The SS is configured:

- with 2 cells: as in TS 36.508 [94]
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell A power level is set as "serving cell" and cell 24/cell 5 power level is set as "suitable cell"

NOTE: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Automatic eCall over IMS is initiated at the UE

1A-1H) IMS registration according to C.2 is executed.

2-5) Emergency registration according to C.20 is executed.

6) SS waits for UE to send an INVITE request

7) SS sends 600 Busy everywhere.

8-9) UE performs domain selection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM registration if necessary. CS eCall is established and maintained for 5 seconds and then the call is cleared by SS.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			UE is triggered to initiate an automatic eCall	Step 2 in generic procedure 36.508 [94] table 4.5A.27.3-1.
1A-1H			Steps 4-11 in Annex C.2	Steps 3 to 18 in generic procedure in 36.508 [94] table 4.5A.27.3-1. UE attaches to the NW, establishes the default PDN, and performs IMS registration.
2-5			Step 1-4 defined in C.20	Steps 19 to 25 in generic procedure 36.508 [94] table 4.5A.27.3-1. UE establishes the emergency PDN and performs IMS emergency registration.
6			Step 1 defined in C.47	UE sends INVITE along with initial SDP offer and MSD,
7	←		600 Busy everywhere	The SS sends 600 Busy everywhere
			EXCEPTION: The UE performs a domain selection for the emergency call and the UE may transmit EXTENDED SERVICE REQUEST	
8a1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8a2			SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
			EXCEPTION: Either step 9a1 or 9b1 is performed, depending on the value of px_RATComb_Tested	
9a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs domain selection to a cell supporting CS domain (UTRAN) and performs eCall establishment in CS domain together with MM registration	NOTE: RAU procedure can take place in parallel to normal CS call.
9a2			SS configures cell A as a “non-suitable cell”	
9a3			eCall is maintained for 5 seconds	
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration defined in Annex C.46 of TS 34.229-1 can take place	
9a4			eCall is cleared by SS	
9b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs domain selection to a cell supporting CS domain (GERAN cell) and performs eCall establishment in CS domain	
9b2			SS configures cell A as a “non-suitable cell”	
9b3			eCall is maintained for 5 seconds	
9b4			eCall is cleared by SS	
9b5			UE performs MM/GMM registration	

Specific Message Contents

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A21.
Step 7 600 Busy Everywhere message as in Annex A.2.22.

RRCConnectionRelease (step 8a2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (Step 9b5)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

21.16.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for automatic eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

In step 9a1 or 9b1, UE shall send an EMERGENCY SETUP message with the Service Category IE bit 7 = 1 and all other bits are set to 0.

21.17 eCall only mode / Manual initiation / Emergency registration / Abnormal case / IM CN sends a 603 (Decline) / UE performs eCall in CS domain / UTRAN or GERAN

21.17.1 Definition

Test to verify that on reception of reject cause 603 Decline for a manually initiated INVITE for eCall over IMS, UE initiates the eCall in supported CS domain over UTRAN or GERAN.

21.17.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.1]:

If the upper layers request establishment of an IMS emergency call of the manually initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.manual" as specified in RFC 8147 [244].

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.automatic" as specified in RFC 8147 [244].

NOTE: The manually initiated eCall type of emergency service is used when the eCall IMS emergency session is invoked with user input. The automatically initiated eCall type of emergency service is used if the eCall IMS emergency session is invoked without user input.

[TS 24.229, clause 5.1.6.11.2]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

   a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

   b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

   c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

…

3) if the UE receives a 486 (Busy Here), 600 (Busy Everywhere) or 603 (Decline) response to the INVITE request containing:

   a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

      i) a "received" attribute set to "true"; and

      ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

   then the UE shall consider the initial MSD transmission as successful and shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B]; and

4) in all other cases, the UE shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B].

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.11.1 and 5.1.6.11.2.

21.17.3 Test purpose

1) To verify that the UE is able to handle 603 (Decline) SIP error message for an automatically initiated INVITE for eCall over IMS; and

2) To verify that the UE is able to establish legacy eCall in CS domain in UTRAN or GERAN system after receiving 603 (Decline) SIP error message.

21.17.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall Only subscription.

The UE is switched on not registered to IMS services.

The SS is configured:

- with 2 cells: as in TS 36.508 [94]
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell A power level is set as "serving cell" and cell 24/cell 5 power level is set as "suitable cell"

NOTE: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Manual eCall over IMS is initiated at the UE

1A-1H) IMS registration according to C.2 is executed.

2-5) IMS Emergency registration according to C.20 is executed.

6) SS waits for UE to send an INVITE request

7) SS sends 603 Decline.

8-9) UE performs domain selection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM registration if necessary.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			UE is triggered to initiate a manual eCall	Step 2 in generic procedure 36.508 [94] table 4.5A.27.3-1.
1A-1H			Steps 4-11 in Annex C.2	Steps 3 to 18 in generic procedure 36.508 [94] table 4.5A.27.3-1. UE attaches to the NW, establishes the default PDN, and performs IMS registration.
2-5			Step 1-4 defined in C.20	Steps 19 to 25 in generic procedure 36.508 [94] table 4.5A.27.3-1. UE establishes the emergency PDN and performs IMS emergency registration.
6			Step 1 defined in C.47	UE sends INVITE along with initial SDP offer and MSD,
7	←		603 Decline	The SS sends 603 Decline
			EXCEPTION: The UE performs a domain selection for the emergency call and the UE may transmit EXTENDED SERVICE REQUEST	
8a1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8a2			SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
			EXCEPTION: Either step 9a1 or 9b1 is performed, depending on the value of px_RATComb_Tested	
9a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs domain selection to a cell supporting CS domain (UTRAN) and performs eCall establishment in CS domain together with MM registration	NOTE: RAU procedure can take place in parallel to normal CS call.
9a2			SS configures cell A as a “non-suitable cell”	
9a3			eCall is maintained for 5 seconds	
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration defined in Annex C.46 of TS 34.229-1 can take place	
9a4			eCall is cleared by SS	
9b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs domain selection to a cell supporting CS domain (GERAN cell) and performs eCall establishment in CS domain	
9b2			SS configures cell A as a “non-suitable cell”	
9b3			eCall is maintained for 5 seconds	
9b4			eCall is cleared by SS	
9b5			UE performs MM/GMM registration	

Specific Message Contents

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A21
Step 7 603 Decline message as in Annex A.2.23.

RRCConnectionRelease (step 8a2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (Step 9b5)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

21.17.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for automatic eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

In step 9a1 or 9b1, UE shall send an EMERGENCY SETUP message with the Service Category IE bit 6 = 1 and all other bits are set to 0.

21.18 eCall only mode / Automatic initiation / Emergency registration / Abnormal case / IM CN sends a 603 (Decline) / UE performs eCall in CS domain / UTRAN or GERAN

21.18.1 Definition

Test to verify that on reception of reject cause 603 Decline for an automatically initiated INVITE for eCall over IMS, UE initiates the eCall in supported CS domain over UTRAN or GERAN.

21.18.2 Conformance requirement

[TS 24.229, clause 5.1.6.11.1]:

If the upper layers request establishment of an IMS emergency call of the manually initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.manual" as specified in RFC 8147 [244].

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service, the service URN shall be "urn:service:sos.ecall.automatic" as specified in RFC 8147 [244].

NOTE: The manually initiated eCall type of emergency service is used when the eCall IMS emergency session is invoked with user input. The automatically initiated eCall type of emergency service is used if the eCall IMS emergency session is invoked without user input.

[TS 24.229, clause 5.1.6.11.2]:

If the upper layers request establishment of an IMS emergency call of the automatically initiated eCall type of emergency service or of the manually initiated eCall type of emergency service and if allowed by IP-CAN specific annex, the UE shall send an INVITE request as specified in the procedures in subclause 5.1.6.8 with the following additions:

1) the UE shall set the Request-URI to "urn:service:sos.ecall.automatic" or "urn:service:sos.ecall.manual"; and

2) if the IP-CAN indicates the eCall support indication, the UE shall:

   a) insert a multipart/mixed body containing an "application/EmergencyCallData.eCall.MSD" MIME body part as defined in RFC 8147 [244], containing the MSD not exceeding 140 bytes and encoded in binary ASN.1 PER as specified in CEN EN 15722:2015 [245] and include a Content-Disposition header field with a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

   b) insert an Accept header field indicating the UE is willing to accept an "application/EmergencyCallData.Control+xml" MIME type as defined in RFC 8147 [244]; and

   c) insert a Recv-Info header field set to "EmergencyCallData.eCall.MSD" as defined in RFC 8147 [244].

NOTE: Further content for the INVITE is as defined in RFC 8147 [244].

Then the UE shall proceed as follows:

…

3) if the UE receives a 486 (Busy Here), 600 (Busy Everywhere) or 603 (Decline) response to the INVITE request containing:

   a) a multipart/mixed body containing an "application/EmergencyCallData.Control+xml" MIME body part as defined in RFC 8147 [244] with an "ack" element containing:

      i) a "received" attribute set to "true"; and

      ii) a "ref" attribute set to the Content-ID of the MIME body part containing the MSD sent by the UE;

   then the UE shall consider the initial MSD transmission as successful and shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B]; and

4) in all other cases, the UE shall perform domain selection to re-attempt the eCall as specified in 3GPP TS 23.167 [4B].

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.6.11.1 and 5.1.6.11.2.

21.18.3 Test purpose

1) To verify that the UE is able to handle 603 (Decline) SIP error message for an automatically initiated INVITE for eCall over IMS; and

2) To verify that the UE is able to establish legacy eCall in CS domain in UTRAN or GERAN system after receiving 603 (Decline) SIP error message.

21.18.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC with eCall Only subscription.

The UE is switched on not registered to IMS services.

The SS is configured:

- with 2 cells: as in TS 36.508 [94]
- E-UTRAN cell A
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell A power level is set as “serving cell” and cell 24/cell 5 power level is set as “suitable cell”

NOTE: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Automatic eCall over IMS is initiated at the UE

1A-1H) IMS registration according to C.2 is executed.

2-5) Emergency registration according to C.20 is executed.

6) SS waits for UE to send an INVITE request

7) SS sends 603 Decline.

8-9) UE performs domain selection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and initiates CS domain emergency call with MM registration if necessary. CS eCall is established and maintained for 5 seconds and then the call is cleared by SS.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			UE is triggered to initiate an automatic eCall	Step 2 in generic procedure 36.508 [94] table 4.5A.27.3-1.
1A-1H			Steps 4-11 in Annex C.2	Steps 3 to 18 in generic procedure in 36.508 [94] table 4.5A.27.3-1. UE attaches to the NW, establishes the default PDN, and performs IMS registration.
2-5			Step 1-4 defined in C.20	Steps 19 to 25 in generic procedure 36.508 [94] table 4.5A.27.3-1. UE establishes the emergency PDN and performs IMS emergency registration.
6			Step 1 defined in C.47	UE sends INVITE along with initial SDP offer and MSD,
7	←		603 Decline	The SS sends 603 Decline
			EXCEPTION: The UE performs a domain selection for the emergency call and the UE may transmit EXTENDED SERVICE REQUEST	
8a1	→		EXTENDED SERVICE REQUEST	If CS Fallback is performed, the UE sends service request with Service type set to *mobile originating CS fallback emergency call* as defined in 24.301 clause 9.9.3.27
8a2			SS releases the RRC connection	SS waits for two seconds before sending RRC connection release. UE state is changed from RRC_CONNECTED to RRC_IDLE, and UE is redirected to UTRAN/GERAN (if supported)
			EXCEPTION: Either step 9a1 or 9b1 is performed, depending on the value of px_RATComb_Tested	
9a1			IF px_RATComb_Tested = EUTRA_UTRA UE performs domain selection to a cell supporting CS domain (UTRAN) and performs eCall establishment in CS domain together with MM registration	NOTE: RAU procedure can take place in parallel to normal CS call.
9a2			SS configures cell A as a “non-suitable cell”	
9a3			eCall is maintained for 5 seconds	
			EXCEPTION: Depending on the UE implementation, the generic test procedure for mobile initiated IMS SIP re-registration defined in Annex C.46 of TS 34.229-1 can take place	
9a4			eCall is cleared by SS	
9b1			IF px_RATComb_Tested = EUTRA_GERAN UE performs domain selection to a cell supporting CS domain (GERAN cell) and performs eCall establishment in CS domain	
9b2			SS configures cell A as a “non-suitable cell”	
9b3			eCall is maintained for 5 seconds	
9b4			eCall is cleared by SS	
9b5			UE performs MM/GMM registration	

Specific Message Contents

Step 6 as specified in annex C.47, which is referring to A.2.1 default message content of INVITE with condition A21
Step 7 603 Decline message as in Annex A.2.23.

RRCConnectionRelease (step 8a2)

Derivation Path: 36.508 Table 4.6.1-15			
Information Element	**Value/remark**	**Comment**	**Condition**
RRCConnectionRelease ::= SEQUENCE {			
criticalExtensions CHOICE {			
c1 CHOICE {			
rrcConnectionRelease-r8 SEQUENCE {			
redirectedCarrierInfo ::= CHOICE {			
utra-FDD	Downlink UARFCN of cell 5		UTRA-FDD
_utra-TDD	Downlink UARFCN of cell 5		UTRA-TDD
geran	ARFCN of cell 24		GERAN
}			
}			

ROUTING AREA UPDATE ACCEPT (Step 9b5)

Use the default message with the following specific contents

Derivation path: 36.508, Table 4.7B.2-2			
Information Element	**Value/Remark**	**Comment**	**Condition**
PDP context status	0	NSAPI(0) - NSAPI(15) is set to 0, which means that the SM state of all PDP contexts is PDP-INACTIVE	

21.18.5 Test requirements

In step 6, UE shall transmit INVITE with all applicable headers for automatic eCall over IMS.

In step 6, UE shall transmit MSD in the INVITE.

In step 9a1 or 9b1, UE shall send an EMERGENCY SETUP message with the Service Category IE bit 7 = 1 and all other bits are set to 0.

22 Session Timer

22.1 MO Call – UE is able to refresh the session

22.1.1 Definition

Test to verify that a UE supporting and using Session timer as described in RFC 4028 [146], and configured to be the refresher and triggered to perform an IMS mobile originated voice call when using IMS Multimedia Telephony with preconditions, correctly negotiates the Session-Expires header, processes received 422 Session Interval Too Small responses, and keeps the session alive as negotiated. This process is described in IR.92 [133] clause 2.2.8, RFC 4028 [146] sections 7.1-7.4 and 3GPP TS 24.229 [10], clause 5.1.2A.1.1.

22.1.2 Conformance requirement

[TS 24.229 clause 5.1.2A.1.1]

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229 clause 5.2.7.2]

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

[TS 24.229 clause 5.2.7.3]

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

[TS 24.229 clause 5.4.5.3]

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1.1, 5.2.7.2, 5.2.7.3, and 5.4.5.3.

22.1.3 Test purpose

1) To verify that, when setting up an MO call, the UE performs correct exchange of SIP protocol signalling messages for Session Timer extension; and

2) To verify that within SIP signalling the UE is able to handle 422 Session Interval Too Small responses by retrying the initial INVITE request (as described by RFC 4028 [10], section 7.4); and

3) To verify that the UE is able to refresh the session using UPDATE based on the session expiration value negotiated in SIP signalling during session set up; and

4) To verify that the UE is able to keep the session active during session refreshes until released; and

5) To verify that the UE does not change the role of refresher during session refreshes.

22.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction UE	Direction SS	Message	Comment
1			Make the UE attempt an IMS speech call	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
2	→		INVITE	UE sends INVITE as described in C.21, step 2, with either the Session-Expires value set to 1800 or no Session-Expires header.
3				
-			EXCEPTION: Steps 4a0 to 4a7 describe behaviour that depends on UE capability: the "lower case letter" identifies a step sequence that takes place if the UE included Session-Expires in step 2	
4a0	←		100 Trying	SS sends 100 Trying response.
4a1	←		422 Session Interval Too Small	SS sends 422 Session Interval Too Small response with Min-SE value of 1860.
4a2	→		ACK	UE sends ACK.
4a3	→		INVITE	UE sends INVITE with Min-SE value and Session-Expires value being 1860.
4a4	←		100 Trying	SS sends 100 Trying response.
4a5	←		422 Session Interval Too Small	SS sends 422 Session Interval Too Small response with Min-SE value of 1920.
4a6	→		ACK	UE sends ACK.
4a7	→		INVITE	UE sends INVITE with Min-SE value and Session-Expires value being 1920.
5-13			Steps 3-11 defined in annex C.21	
14	←		200 OK	SS sends 200 OK for INVITE with negotiated Session-Expires value set to 1920 and refresher value set to uac.
15	→		ACK	UE sends ACK.
16	→		UPDATE	960 seconds after step 15, UE sends an UPDATE request to refresh the session.
17	←		200 OK	SS sends 200 OK for UPDATE.
18	→		UPDATE	960 seconds after step 17, UE sends an UPDATE request to refresh the session.
19	←		200 OK	SS sends 200 OK for UPDATE.
20-23			Steps defined in annex C.33	SS releases the call.

Specific Message Contents

INVITE (Step 2)

Use the default Message "INVITE" in Annex C.21 with conditions A1, A3, A4 and A26 and the following exceptions:

Header/param	Value/remark
Session-Expires	(if present)
delta-seconds	1800
refresher	uac (if present)

422 Session Interval Too Small (Step 4a1)

Use the default Message "422 Session Interval Too Small" in Annex A.2.24 with the following exceptions:

Header/param	Value/remark
Min-SE	
delta-seconds	1860

INVITE (Step 4a3)

Use the default Message "INVITE" in Annex C.21 with conditions A1, A3, A4 and A26 and the following exceptions:

Header/param	Value/remark
Call-ID	
callid	The same value as in INVITE in Step 2
From	
addr-spec	The same value as in INVITE in Step 2
tag	The same value as in INVITE in Step 2
To	
addr-spec	The same value as in INVITE in Step 2
CSeq	
value	The value sent in the INVITE in step 2, incremented by one
Session-Expires	
delta-seconds	1860
Min-SE	
delta-seconds	1860

422 Session Interval Too Small (Step 4a5)

Use the default Message 422 Session Interval Too Small in Annex A.2.24 with the following exceptions:

Header/param	Value/remark
Min-SE	
delta-seconds	1920

INVITE (Step 4a7)

Use the default Message "INVITE" in Annex A.2.1 with conditions A1, A3, A4 and A26 and the following exceptions:

Header/param	Value/remark
Call-ID	
callid	The same value as in INVITE in Step 4a3
From	
addr-spec	The same value as in INVITE in Step 4a3
tag	The same value as in INVITE in Step 4a3
To	
addr-spec	The same value as in INVITE in Step 4a3
CSeq	
value	The value sent in the INVITE in step 4a3, incremented by one
Session-Expires	
delta-seconds	1920
Min-SE	
delta-seconds	1920

183 Session Progress (Step 6)

Use the default Message "183 Session Progress for INVITE" in Annex A.2.3 with condition A1 and the following exceptions:

Header/param	Value/remark
Allow	INVITE, UPDATE, PRACK, ACK, OPTIONS, CANCEL, BYE

200 OK (Step 14)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A1 and A10 and the following exceptions:

Header/param	Value/remark
Allow	INVITE, UPDATE, PRACK, ACK, OPTIONS, CANCEL, BYE
Require	timer
Supported	timer
Session-Expires	
delta-seconds	1920
refresher	uac
Min-SE	
delta-seconds	1920

UPDATE (Steps 16 and 18)

Use the default Message "UPDATE" in Annex A.2.5 with condition A1 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires	
delta-seconds	1920
refresher	uac
Min-SE	
delta-seconds	1920
Content-Type	any value if present

200 OK (Steps 17 and 19)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A1 and A10 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires delta-seconds refresher	 1920 uac
Min-SE delta-seconds	 1920

22.2 MO Call – Remote end is refresher

22.2.1 Definition

Test to verify that a UE supporting and using Session timer as described in RFC 4028 [146], and configured to not ask to be the refresher and triggered to perform an IMS mobile originated voice call when using IMS Multimedia Telephony with preconditions, accepts the Session-Expires header provided by the remote UE, accepts keep alive requests, and terminates the session upon time. This process is described in TS 24.229 [10], IR.92 [133] clause 2.2.8 and RFC 4028 [146] sections 7.1-7.4.

22.2.2 Conformance requirement

[TS 24.229 clause 5.1.2A.1.1]

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229 clause 5.2.7.2]

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

[TS 24.229 clause 5.2.7.3]

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

[TS 24.229 clause 5.4.5.3]

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1.1, 5.2.7.2, 5.2.7.3, and 5.4.5.3.

22.2.3 Test purpose

1) To verify that, when setting up an MO call, the UE performs correct exchange of SIP protocol signalling messages for Session Timer extension; and

2) To verify that within SIP signalling the UE is able to handle incoming UPDATE requests that are intended to keep the session alive (as described by RFC 4028 [10], section 10) and respond accordingly; and

3) To verify that the UE does not change the role of refresher during session refreshes; and

4) To verify that the UE will end the call upon session expiration.

22.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS speech call	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
2	→		INVITE	UE sends INVITE as described in C.21, step 2.
3-11			Steps 3-11 defined in annex C.21	
12	←		200 OK	SS sends 200 OK for INVITE with Session-Expires value set to 1800 and refresher value set to uas.
13	→		ACK	UE sends ACK.
14	←		UPDATE	900 seconds after step 12, SS sends an UPDATE request to refresh the session.
15	→		200 OK	UE sends 200 OK for UPDATE.
16-19			Steps 2-5 defined in annex C.32	1800 seconds after step 15, UE releases the call due to session expiring.

Specific Message Contents

INVITE (Step 2)

Use the default Message "INVITE" in Annex C.21 with conditions A1, A3, A4 and A26 and the following exceptions:

Header/param	Value/remark
Session-Expires	(if present)
delta-seconds	1800
refresher	not present

200 OK (Step 12)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A1 and A10 and the following exceptions:

Header/param	Value/remark
Require	timer
Supported	timer
Session-Expires delta-seconds refresher	 1800 uas

UPDATE (Step 14)

Use the default Message "UPDATE" in Annex A.2.5 with condition A3 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires delta-seconds refresher	 1800 uac
Content-Type	not present

200 OK (Step 15)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A1 and A10 and the following exceptions:

Header/param	Value/remark
Require	timer
Session-Expires delta-seconds refresher	 1800 uac

22.3 MO Call – Remote end does not support Session Timer

22.3.1 Definition

Test to verify that a UE supporting and using Session Timer as described in RFC 4028 [146], configured to use Session Timer for its purposes when remote end does not support Session Timer (and no proxies in between mandate its usage), during an IMS mobile originated voice call when using IMS Multimedia Telephony with preconditions, correctly sets the Session-Expires interval and chooses refresher when the remote UE does not support the Session Timer extension, becomes refresher of the session, generates periodic session refreshes and keeps the session alive until termination. This process is described in RFC 4028 [146] sections 7.1-7.4.

22.3.2 Conformance requirement

[TS 24.229 clause 5.1.2A.1.1]

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229 clause 5.2.7.2]

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

[TS 24.229 clause 5.2.7.3]

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

[TS 24.229 clause 5.4.5.3]

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1.1, 5.2.7.2, 5.2.7.3, and 5.4.5.3.

22.3.3 Test purpose

1) To verify that, when setting up an MO call, the UE performs correct exchange of SIP protocol signalling messages for Session Timer extension; and

2) To verify that, within SIP signalling, the UE correctly sets Session Expires Interval and becomes refresher when remote end does not indicate Session Timer Support in 200 OK response to initial INVITE (as described by RFC 4028 [10], section 7.2); and

3) To verify that the UE generates periodic session refreshes and is able to keep the session active until released; and

4) To verify that the UE does not change the role of refresher during session refreshes.

22.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS speech call	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
2	→		INVITE	UE sends INVITE as described in C.21, step 2, indicating support for Session Timer, with either the Session-Expires value set to 1800 or no Session-Expires header
3-11			Steps 3-11 defined in annex C.21	
12	←		200 OK	SS sends 200 OK for INVITE, without timer tag in Supported and Require headers and without Session-Expires header
13	→		ACK	UE sends ACK.
14	→		UPDATE	900 seconds after step 13, UE sends an UPDATE request to refresh the session.
15	←		200 OK	SS sends 200 OK for UPDATE, without timer tag in Supported and Require headers and without Session-Expires header
16	→		UPDATE	900 seconds after step 15, UE sends an UPDATE request to refresh the session.
17	←		200 OK	SS sends 200 OK for UPDATE, without timer tag in Supported and Require headers and without Session-Expires header
18-21			Steps defined in annex C.33	SS releases the call.

Specific Message Contents

INVITE (Step 2)

Use the default Message "INVITE" in Annex C.21 with conditions A1, A3, A4 and A26 and the following exceptions:

Header/param	Value/remark
Session-Expires	(if present)
delta-seconds	1800
refresher	uac (if present)

183 Session Progress (Step 4)

Use the default Message "183 Session Progress for INVITE" in Annex A.2.3 with condition A1 and the following exceptions:

Header/param	Value/remark
Allow	INVITE, UPDATE, PRACK, ACK, OPTIONS, CANCEL, BYE

200 OK (Step 12)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A1 and A10 and the following exceptions:

Header/param	Value/remark
Allow	INVITE, UPDATE, PRACK, ACK, OPTIONS, CANCEL, BYE

UPDATE (Steps 14 and 16)

Use the default Message "UPDATE" in Annex A.2.5 with condition A1 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires	
delta-seconds	1800
refresher	uac
Content-Type	any value if present

22.4 MO Call – Remote end supports but does not use Session Timer

22.4.1 Definition

Test to verify that a UE supporting and using Session Timer as described in RFC 4028 [146], configured to indicate Session Timer support, when remote end supports but does not want to use Session Timer (and no proxies in between mandate its usage), during an IMS mobile originated voice call when using IMS Multimedia Telephony with preconditions, turns-off the use of Session Timer for the session hence does not generate periodic session refresh and keeps the session alive until termination. This process is described in IR.92 [133] clause 2.2.8, RFC 4028 [146] sections 7.1-7.4.

22.4.2 Conformance requirement

[TS 24.229 clause 5.1.2A.1.1]

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229 clause 5.2.7.2]

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

[TS 24.229 clause 5.2.7.3]

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

[TS 24.229 clause 5.4.5.3]

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1.1, 5.2.7.2, 5.2.7.3, and 5.4.5.3.

22.4.3 Test purpose

1) To verify that, when setting up an MO call, the UE performs correct exchange of SIP protocol signalling messages for Session Timer extension; and

2) To verify that, within SIP signalling, the UE correctly indicates Session Timer support by including timer tag in Supported header (as described by RFC 4028 [10], section 7.2); and

3) To verify that the UE turns off the use of Session Timer extension for the session upon receiving 200 OK response from the remote end indicating Session Timer support with timer tag in Supported header but without Session-Expires header; and

4) To verify that the UE does not generate any periodic session refreshes and is able to keep the session active until released.

22.4.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS speech call using a Session-Expires	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
2	→		INVITE	UE sends INVITE as described in C.21, step 2, indicating support for Session Timer, with either the Session-Expires value set to 1800 or no Session-Expires header
3-11			Steps 3-11 defined in annex C.21	
12	←		200 OK	SS sends 200 OK for INVITE, with timer tag in Supported header but without Session-Expires header
13	→		ACK	UE sends ACK.
14-17			Steps defined in annex C.33	1860 seconds after step 13, SS releases the call.

Specific Message Contents

INVITE (Step 2)

Use the default Message "INVITE" in Annex C.21 with conditions A1, A3, A4 and A26 and the following exceptions:

Header/param	Value/remark
Session-Expires	(if present)
delta-seconds	1800
refresher	uac (if present)

200 OK (Step 12)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A1 and A10 and the following exceptions:

Header/param	Value/remark
Supported	timer

22.5 MT Call – Remote end supports but does not send Session-Expires

22.5.1 Definition

Test to verify that a UE supporting and using Session timer as described in RFC 4028 [146], during mobile terminated speech call setup when using IMS Multimedia Telephony, correctly responds to MT INVITE not having Session-Expires header, chooses remote end as refresher, responds to periodic refreshes, keeps session active until refresh requests are received from remote end, and terminates session upon not receiving session refresh request after session expiration interval. This process is described in IR.92 [133] clause 2.2.8 and RFC 4028 [146] sections 9.

22.5.2 Conformance requirement

[TS 24.229 clause 5.1.2A.1.1]

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229 clause 5.2.7.2]

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

[TS 24.229 clause 5.2.7.3]

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

[TS 24.229 clause 5.4.5.3]

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1.1, 5.2.7.2, 5.2.7.3, and 5.4.5.3.

22.5.3 Test purpose

1) To verify that, during an MT call setup, the UE performs correct exchange of SIP protocol signalling messages for Session Timer extension; and

2) To verify that within SIP signalling the UE correctly selects the remote end as refresher for the session where remote end indicates support with "timer" tag in Supported header but does not include Session-Expires header in INVITE request; and

3) To verify that the UE keeps the session active during session refreshes from remote end and is able to respond to periodic refresh UPDATE requests; and

4) To verify that the UE is able to terminate the session upon not receiving periodic session refresh request from remote end.

22.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipp5ed into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to 26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE as described in C.11, step 1.
2-11			Steps 3-11A defined in annex C.11	
12	→		200 OK	UE sends 200 OK for INVITE with Session-Expires value set to 1800 and refresher value set to uac.
13	←		ACK	SS sends ACK.
14	←		UPDATE	900 seconds after step 12, SS sends an UPDATE request to refresh the session.
15	→		200 OK	UE sends 200 OK for UPDATE.
16-19			Steps 2-5 defined in annex C.32	1800 seconds after step 15, UE releases the call due to session expiry.

Specific Message Contents

INVITE (Step 1)

Use the default message “INVITE for MT Call” in annex A.2.9 with conditions A1, A3, and A4.

200 OK (Step 12)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A2 and A11 and the following exceptions:

Header/param	Value/remark
Require	timer
Session-Expires	
delta-seconds	1800
refresher	uac

UPDATE (Step 14)

Use the default Message "UPDATE" in Annex A.2.5 with condition A3 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires delta-seconds refresher	 1800 uac
Content-Type	not present

200 OK (Steps 15)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A2 and A11 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires delta-seconds refresher	 1800 uac

22.6 MT Call – Remote end sends Session-Expires but does not choose refresher

22.6.1 Definition

Test to verify that a UE supporting and using Session timer as described in RFC 4028 [146], during mobile terminated speech call setup when using IMS Multimedia Telephony, chooses remote end as refresher, responds to periodic refreshes and keeps session active until refresh requests are received from remote end. This process is described in IR.92 [133] clause 2.2.8 and RFC 4028 [146] section 9.

22.6.2 Conformance requirement

[TS 24.229 clause 5.1.2A.1.1]

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229 clause 5.2.7.2]

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

[TS 24.229 clause 5.2.7.3]

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

[TS 24.229 clause 5.4.5.3]

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1.1, 5.2.7.2, 5.2.7.3, and 5.4.5.3.

22.6.3 Test purpose

1) To verify that, during a MT call setup, the UE performs correct exchange of SIP protocol signalling messages for Session Timer extension; and

2) To verify that the UE correctly responds with 200 OK with Session-Expires value received in MT INVITE and correctly selects the remote end as refresher for the session; and

3) To verify that the UE keeps the session active during session refreshes from remote end and able to respond to periodic refresh UPDATE requests.

22.6.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to 26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE as described in C.11, step 2, with timer tag set in Supported header and Session-Expires value set to 1800.
2-11			Steps 3-11A defined in annex C.11	
12	→		200 OK	UE sends 200 OK for INVITE with Session-Expires value set to 1800 and refresher value set to uac.
13	←		ACK	SS sends ACK.
14	←		UPDATE	900 seconds after step 17, SS sends an UPDATE request to refresh the session.
15	→		200 OK	UE sends 200 OK for UPDATE.
16-19			Steps defined in annex C.33	SS releases the call.

Specific Message Contents

INVITE (Step 1)

Use the default message “INVITE for MT Call” in annex A.2.9 with conditions A1, A3, A4 and following exceptions:

Header/param	Value/remark
Session-Expires	
delta-seconds	1800

200 OK (Step 12)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A2 and A11 and the following exceptions:

Header/param	Value/remark
Require	timer
Session-Expires	
delta-seconds	1800
refresher	uac

UPDATE (Step 14)

Use the default Message "UPDATE" in Annex A.2.5 with condition A3 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires	
delta-seconds	1800
Refresher	uac
Content-Type	not present

200 OK (Steps 15)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A2 and A11 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires	
delta-seconds	1800
refresher	uac

22.7 MT Call – Remote end chooses UE as refresher

22.7.1 Definition

Test to verify that a UE supporting and using Session timer as described in RFC 4028 [146], during mobile terminated speech call setup when using IMS Multimedia Telephony, correctly responds to MT INVITE with Session-Expires and refresher set as uas, becomes refresher of the session and does periodic refreshes and keeps session active during session refreshes. This process is described in IR.92 [133] clause 2.2.8 and RFC 4028 [146] section 9.

22.7.2 Conformance requirement

[TS 24.229 clause 5.1.2A.1.1]

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229 clause 5.2.7.2]

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

[TS 24.229 clause 5.2.7.3]

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

[TS 24.229 clause 5.4.5.3]

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1.1, 5.2.7.2, 5.2.7.3, and 5.4.5.3.

22.7.3 Test purpose

1) To verify that, during an MT call setup, the UE performs correct exchange of SIP protocol signalling messages for Session Timer extension; and

2) To verify that, within SIP signalling, the UE responds to MT INVITE correctly where remote end has indicated session timer support and chosen UE as refresher by setting refresher as uas in Session-Expires header; and

3) To verify that, the UE becomes refresher of the session and generate periodic session refresh with Re-INVITE requests since UPDATE method is not listed in Allow header of MT INVITE; and

4) To verify that, the UE keeps the session active during session refreshes.

22.7.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipp5ed into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to 26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE as described in C.11, step 1, with Session-Expires value set to 1800 and refresher set to uas.
2-11			Steps 3-11A defined in annex C.11	
12	→		200 OK	UE sends 200 OK for INVITE with Session-Expires value set to 1800 and refresher value set to uas.
13	←		ACK	SS sends ACK.
14	→		INVITE	900 seconds after step 13, UE sends an INVITE request to refresh the session.
15	←		200 OK	SS sends 200 OK for INVITE.
16	→		ACK	UE sends ACK.
17	→		INVITE	900 seconds after step 16, UE sends an INVITE request to refresh the session.
18	←		200 OK	SS sends 200 OK for INVITE.
19	→		ACK	UE sends ACK.
20-23			Steps defined in annex C.33	SS releases the call.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with conditions A1, A3, A4 and following exceptions:

Header/param	Value/remark
Allow	INVITE, ACK, OPTIONS, CANCEL, BYE
Session-Expires	
delta-seconds	1800
refresher	uas

200 OK (Step 12)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A2 and A11 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires	
delta-seconds	1800
refresher	uas

INVITE (Step 14 and 17)

Use the default Message "INVITE" in Annex A.2.1 with conditions A5 and A26 and the following exceptions:

Header/param	Value/remark
Session-Expires delta-seconds refresher	 1800 uac
Content-Type media-type	 application/sdp
Content-Length value	 length of message-body
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(origin) [NOTE 1] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) if present - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: Any media, if present Note 1: Same origin as in last SDP sent by the UE.

200 OK (Steps 15 and 18)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A2 and A11 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires delta-seconds refresher	 1800 uac

22.8 MT Call – Remote end does not support Session Timer

22.8.1 Definition

Test to verify that a UE supporting and using Session timer as described in RFC 4028 [146], when receiving INVITE without Session Timer will instrument and use a Session Timer for its own purpose. This process is described in RFC 4028 [146] sections 7.1-7.4.

22.8.2 Conformance requirement

[TS 24.229 clause 5.1.2A.1.1]

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229 clause 5.2.7.2]

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

[TS 24.229 clause 5.2.7.3]

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.
NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

[TS 24.229 clause 5.4.5.3]

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

Reference(s)

3GPP TS 24.229 [10], clauses 5.1.2A.1.1, 5.2.7.2, 5.2.7.3, and 5.4.5.3.

22.8.3 Test purpose

1) To verify that, during an MT call setup, the UE performs correct exchange of SIP protocol signalling messages for Session Timer extension; and

2) To verify that, within SIP signalling, the UE responds to MT INVITE correctly where remote end has not indicated session timer support by setting refresher as uas in Session-Expires header; and

3) To verify that, the UE becomes refresher of the session and generates periodic session refresh UPDATE requests; and

4) To verify that, the UE keeps the session active during session refreshes.

22.8.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to 26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE as described in C.11, step 1, without support for Session-Timer.
2-11			Steps 3-11A defined in annex C.11	
12	→		200 OK	UE sends 200 OK for INVITE with Session-Expires value set to 1800 and refresher value set to uas.
13	←		ACK	SS sends ACK.
14	→		UPDATE	900 seconds after step 13, UE sends an UPDATE request to refresh the session.
15	←		200 OK	SS sends 200 OK for UPDATE.
16-19			Steps 1-4 defined in annex C.33	SS ends the call.

Specific Message Contents

INVITE (Step 1)

Use the default Message "INVITE" in Annex C.11 with conditions A1, A3, A4 and A7 and the following exceptions:

Header/param	Value/remark
Allow	INVITE, UPDATE, PRACK, ACK, OPTIONS, CANCEL, BYE

200 OK (Step 12)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A2 and A11 and the following exceptions:

Header/param	Value/remark
Session-Expires	
delta-seconds	1800
refresher	uas

UPDATE (Step 14)

Use the default Message "UPDATE" in Annex A.2.5 with condition A3 and the following exceptions:

Header/param	Value/remark
Supported	timer
Session-Expires	
delta-seconds	1800
refresher	uac
Content-Type	any value if present

200 OK (Steps 15)

Use the default Message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 with conditions A1 and A10.

Annex A (normative): Default Messages

For all the message definitions below, the acceptable order and syntax of headers and fields within these headers must be according to IETF RFCs where those headers have been defined. Typically the order of headers is not significant, but there are well defined exceptions (like Via, Route, Record-Route headers, and SDP lines) where the order is important.

The contents of the messages described in the present Annex is not complete - only the fields, headers, and SDP lines required to be checked or generated by SS are listed here. The messages sent by the UE may contain additional parameters, fields, headers, and SDP lines which are not checked and must thus be ignored by SS.

Values prefixed with px_ will be implemented in the TTCN with a PIXIT.

Values shown in *italics* shall be used in the messages as such.

Conditions listed in the "Cond" column in the tables of the present Annex have different purposes.

- When a condition is listed on the same line as the name of header, the presence of this header is:
    - optional when this condition applies and the condition is appended by the (o) tag: e.g. 'A2(o)'.
    - mandatory when this condition applies and the condition is not appended: e.g. 'A2'.

NOTE 1: This includes negative Boolean expressions, i.e. a "NOT expression" mandates presence of the header whenever the condition does not apply. Still the UE is allowed to include the header under such negative Boolean expression – it is just not required to do so.

- The absence of a header or parameter is checked under a condition listed on the same line as the name of the header/parameter when the Value/remark column carries the explicit phrase "not present".
- When no condition is listed on the same line as the name of a header, presence or absence of the header is regulated under all conditions, i.e., when the Value/remark column states absence of the header it is absent under all conditions. Otherwise it is present under all conditions.
- When a condition is listed on the same line as an indented subentry of a header, i.e., a parameter, the corresponding entry in the "Value/remark" column imposes a requirement on the value of this parameter when this condition applies.
- When no condition is listed on the same line as a parameter and there are line(s) for the same parameter carrying condition(s), the meaning is that the former line constitutes a default and the latter line(s) constitute special regulations under the specific condition(s).

NOTE 2: In above bullet points, "header" is used for the boldface entries in the Header/param columns starting a sub table, e.g., Request-Line**,** Route, and Message-body, even though not all these terms technically represent SIP headers. Similarly, we use the generic term "parameter" to denote subentries of such "headers".

A.1 Default messages for IMS Registration

A.1.1 REGISTER

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*REGISTER*		
Request-URI		SIP URI formed from home domain name as stored in EF_{DOMAIN} (when using ISIM) or SIP URI formed from home domain name derived from the IMSI (when no ISIM available on the UICC)		
	A14,A15	SIP URI formed from home domain name as preconfigured in the UE		
SIP-Version		*SIP/2.0*		
Route		not present		RFC 3261 [15]
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1,A3, A14,A15	IP address or FQDN, port (optional) and not checked		
	A2	IP address or FQDN and, when using UDP, protected server port of the UE		
response-port	A1,A3	*rport* (when using UDP)		RFC 3581 [96]
via-branch		value starting with '*z9hG4bK'*		
From				RFC 3261 [15]
addr-spec	A1	any IMPU within the set of IMPUs on ISIM (when using ISIM; NOTE 3) or public user identity derived from IMSI (when no ISIM available on the UICC)		
	A2,A15	same public user identity as in initial REGISTER		
	A3 AND NOT A7	public user identity derived from IMSI		
	A7	emergency public user identity (NOTE 4)		
	A14	IMPU preconfigured in the UE		
	A17	same public user identity as in initial REGISTER		
tag		must be present, value not checked		
To				RFC 3261 [15]
addr-spec	A1	any IMPU within the set of IMPUs on ISIM (when using ISIM; NOTE 3) or public user identity derived from IMSI (when no ISIM available on the UICC)		
	A2,A15	same public user identity as in initial REGISTER		
	A3 AND NOT A7	public user identity derived from IMSI		
	A7	emergency public user identity (NOTE 4)		
	A14	IMPU preconfigured in the UE		
	A17	same public user identity as in initial REGISTER		
tag		not present		
Contact				RFC 3261 [15]
addr-spec	A1,A3, A14,A15	SIP URI with IP address or FQDN and indicating either an unprotected port selected by the UE or no port at all		
	A2	SIP URI with IP address or FQDN and protected server port of UE		
	A7	The SIP URI shall contain the *sos* URI parameter		
feature-param	A4 AND A34	*+g.3gpp.icsi-ref="*(comma-separated list of tag-values)*"* with comma-separated list of tag-values containing at least tag-value *urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"* (see NOTE 2,5)		
	A6 AND NOT A7 AND A34	*+g.3gpp.smsip*		
	A10 AND A34	*video*		
	A28 AND (A29 OR A30) AND A34	*audio*		

	A11 AND NOT A7 AND A34	*+g.3gpp.cs2ps-srvcc*	Rel-11	
	A12 AND NOT A7 AND A34	*+g.3gpp.cs2ps-srvcc-alerting*	Rel-11	
	A13 AND NOT A16 AND A34	*+g.3gpp.accesstype="cellular2"*	Rel-11	RFC 3840 [63]
	A13 AND A16 AND A34	*+g.3gpp.accesstype="wlan1"*	Rel-11	RFC 3840 [63]
c-p-instance	A5	*+sip.instance="<urn:gsma:imei*: (gsma-specifier-defined-substring)>" where gsma-specifier-defined-substring shall be the IMEI code of the UE, coded as specified in RFC 7254 [122], without optional parameters	Rel-10	RFC 5627 [61] RFC 7254 [122]
expires		*600000* (if present)		
Expires delta-seconds		present if no expires parameter in Contact header *600000*		RFC 3261 [15]
Require option-tag	A1,A2	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Proxy-Require option-tag	A1,A2	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Supported option-tag	 A5	 *gruu* *path*		RFC 3261 [15] TS 24.229 [10]
CSeq value method	 A1,A3 A14 A2,A15	 must be present, value not checked must be incremented from the previous REGISTER *REGISTER*		RFC 3261 [15]
Call-ID callid		 value not checked		RFC 3261 [15]
Security-Client mechanism-name algorithm protocol mode encrypt-algorithm spi-c spi-s port-c port-s	A1,A2	 *ipsec-3gpp* *hmac-sha-1-96* *esp* (if present) *trans* (if present) *des-ede3-cbc* or *aes-cbc* or *null* SPI number of the inbound SA at the protected client port SPI number of the inbound SA at the protected server port protected client port protected server port		RFC 3329 [21] RFC 4835 [124]
Security-Client	A14,A15	not present		
Security-Verify sec-mechanism	A2 A2	 same value as Security-Server header sent by SS		RFC 3329 [21]
Security-Verify	A1,A3 A14,A15	not present		
Authorization	A1	*Digest*		RFC 2617 [16] RFC 3310 [17]

username	A1	private user identity as stored in EF_{IMPI} (when using ISIM) or private user identity derived from IMSI (when no ISIM available on the UICC)		
realm	A1	home domain name as stored in EF_{DOMAIN} (when using ISIM) or home domain name derived from the IMSI (when no ISIM available on the UICC)		
nonce	A1	set to an empty value		
digest-uri	A1	SIP URI formed from home domain name as stored in EF_{DOMAIN} (when using ISIM) or formed from home domain name derived from the IMSI (when no ISIM available on the UICC)		
response	A1	set to an empty value		
Authorization	A14(o)	Header optional		
username	A14	user identity as preconfigured in the UE		
realm	A14	home domain name as preconfigured in the UE		
nonce	A14	set to an empty value		
digest-uri	A14	preconfigured in the UE		
response	A14	set to an empty value		
Authorization	A2,A15	*Digest*		RFC 2617 [16] RFC 3310 [17]
username	A2	private user identity as stored in EF_{IMPI} (when using ISIM) or private user identity derived from IMSI (when no ISIM available on the UICC)		
	A15	user identity as preconfigured in the UE		
realm	A2,A15	same value as received in the realm directive in the WWW Authenticate header sent by SS		
nonce	A2,A15	same value as in WWW-Authenticate header sent by SS		
opaque	A2,A15	same value as sent by the server in “401 Unauthorized for REGISTER”		
digest-uri	A2	SIP URI formed from home domain name as stored in EF_{DOMAIN} (when using ISIM) or formed from home domain name derived from the IMSI (when no ISIM available on the UICC)		
	A15	SIP URI formed from home domain name as preconfigured in the UE		
qop-value	A2,A15	*auth*		
cnonce-value	A2,A15	value assigned by UE affecting the response calculation		
nonce-count	A2,A15	counter to indicate how many times UE has sent the same value of nonce within successive REGISTER requests, initial value shall be 1		
	A17	value incremented by one for each re-registration request		RFC 2617 [16]
response	A2	response calculated by UE		
	A15	response calculated by UE using password *px_DigestPasswordForSIP*		
algorithm	A2	*AKAv1-MD5*		
	A15	*MD5*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A2,A15, A14(o), A16(o)			RFC 7315 [132] RFC 7913 [154]
access-net-spec	A2 AND A31	access network information for E-UTRAN and, if applicable, the cell ID		
	A14,A15	access network information for Fixed Broadband with access-type field matching “*DLS*” and a "dsl-location" parameter (value not checked)		
	A16	access network information, containing any of “IEEE-802.11”, “IEEE-802.11a”, “IEEE-802.11b”, “IEEE-802.11g” or “IEEE-802-11n”, and i-wlan-node-id parameter containing a MAC address according to TS 24.229 [10], 7.2A.4.2. Value of MAC address not to be checked		
	A2 AND A32	access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	Rel-15	

	A2 AND A33	access network information for UTRAN and, if applicable, the cell ID		
Content-Length value		header shall be present if UE uses TCP to send this message and if there is a message-body length of request body, if such is present		RFC 3261 [15]

Condition	Explanation
A1	Initial unprotected REGISTER (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A2	Subsequent REGISTER sent over security associations (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A3	REGISTER for the case UE supports GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A4	UE supports IMS Multimedia Telephony (MTSI) (A.3A/50 3GPP TS 34.229-2 [5])
A5	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5]). Mandatory from Rel-10 onwards.
A6	UE supports SM-over-IP receiver (A.3A/62 3GPP TS 34.229-2 [5])
A7	Initial unprotected or subsequent REGISTER for emergency registration
A8	Void
A10	UE supports video feature tag (A.12/32 3GPP TS 34.229-2 [5])
A11	UE supports CS to PS SRVCC (A.12/40 3GPP TS 34.229-2 [5])
A12	UE supports CS to PS SRVCC in alerting state (A.12/41 3GPP TS 34.229-2 [5])
A13	UE indicates g.3gpp.accesstype media feature tag in REGISTER (A.12/46 3GPP TS 34.229-2 [5])
A14	Initial REGISTER SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])
A15	Subsequent REGISTER SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])
A16	IMS registration over WLAN
A17	UE initiated IMS re-registration or de-registration (A.12/51 3GPP TS 34.229-2 [5])
A18-A27	Void
A28	UE supports audio media feature tag (A.12/56 3GPP TS 34.229-2 [5])
A29	UE uses E-UTRAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.301 [150], clauses 8.2.1 and 9.9.3.12A
A30	UE uses UTRAN/GERAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.008 [12], clauses 9.4.2 and 10.5.5.23
A31	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A32	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])
A33	UE uses UTRAN access (A.18/2 3GPP TS 34.229-2 [5])
A34	Feature tags in Contact header to be checked. By default this condition is true.

NOTE 1: All choices for applicable conditions are described for each header.

NOTE 2: The "=" may include optional linear white spaces according to the EQUAL definition in chapter 25.1, RFC 3261 [15].

NOTE 3: Public user identity shall be the same for 'From' and 'To'.

NOTE 4: According to TS 24.229 clause 5.1.1.1A and 5.1.6.2 [10] when the UE is using ISIM the emergency public user identity is the first public user identity in the list stored in the ISIM; when there is no ISIM it is the default public user id if the UE successfully performed IMS registration with the IM CN subsystem before, and the temporary user id (derived from IMSI) in all other cases.

NOTE 5: URN is the outcome of the URL encoding ("Percent-Encoding" according to RFC 3986 [129]) of urn:urn-7:3gpp-service.ims.icsi.mmtel.

A.1.2 401 Unauthorized for REGISTER

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *401* *Unauthorized*		RFC 3261 [15]
Via via-parm		 same value as received in REGISTER message		RFC 3261 [15]
To addr-spec tag		 same value as received in REGISTER message common to-tag (register)		RFC 3261 [15]
From addr-spec tag		 same value as received in REGISTER message same value as received in REGISTER message		RFC 3261 [15]
Call-ID callid		 same value as received in REGISTER message		RFC 3261 [15]
CSeq value		 same value as received in REGISTER message		RFC 3261 [15]
WWW-Authenticate realm algorithm qop-value nonce opaque	 A2 A1 A2	*Digest* home domain name as stored in EF_{DOMAIN} or home domain name derived from the IMSI home domain name as preconfigured in the UE *AKAv1-MD5* *MD5* *auth* Base 64 encoding of RAND and AUTN arbitrary value (to be returned by the UE in subsequent REGISTER)		RFC 2617 [16] RFC 3310 [17]
Security-Server mechanism-name algorithm spi-c spi-s port-c port-s Encrypt-algorithm q Mechanism-name algorithm spi-c spi-s port-c port-s encrypt-algorithm q	A1	 *ipsec-3gpp* px_IMS_SecAlgorithm (hmac-md5-96 or hmac-sha-1-96) SPI number of the inbound SA at the protected client port SPI number of the inbound SA at the protected server port protected client port of SS protected server port of SS *des-ede3-cbc* or *aes-cbc* 0.9 *ipsec-3gpp* Algorithm not selected by px_IMS_IPSecAlgorithm (hmac-sha-1-96 or hmac-md5-96) SPI number of the inbound SA at the protected client port SPI number of the inbound SA at the protected server port protected client port of SS protected server port of SS *des-ede3-cbc* or *aes-cbc* *0.7*		RFC 3329 [21]
Security-Server	A2	not present		
Content-Length value		 0		RFC 3261 [15]

Condition	Explanation
A1	IMS Security (A.6a/2 3GPP TS 34.229-2 [5])
A2	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])

A.1.3 200 OK for REGISTER

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*200*		
Reason-Phrase		*OK*		
Via				RFC 3261 [15]
via-parm		same value as received in REGISTER message		
To				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
tag		common to-tag (register)		
From				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
tag		same value as received in REGISTER message		
Call-ID				RFC 3261 [15]
callid		same value as received in REGISTER message		
CSeq				RFC 3261 [15]
value		same value as received in REGISTER message		
Contact				RFC 3261 [15] RFC 5627 [61]
addr-spec		same value as received in REGISTER message		
pub-gruu	A1	Public GRUU as the SIP URI got from the To header of the REGISTER request, together with the gr parameter with an arbitrary value		
temp-gruu	A1	Temporary GRUU with an arbitrary value in the user part and the host part matching with the domain of the To header of the REGISTER and gr parameter without any value		
	A3	not present		
feature-param		same value as received in REGISTER message		
expires		600000		
P-Associated-URI		order of the parameters in this header must be like in the respective rows		RFC 7315 [132]
addr-spec	A2	all the IMPUs within the set of IMPUs on ISIM (NOTE 1), additional associated TEL URI (NOTE 2)		
	A3	emergency public user identity (NOTE 3)		
	A5	IMPU preconfigured in the UE, additional associated TEL URI (NOTE 2)		
Service-Route	A2			RFC 3608 [19]
addr-spec		*scscf.3gpp.org*		
uri-parameter		*lr*		
Path				RFC 3327 [20]
addr-spec		SS P-CSCF address		
uri-parameter		*lr*		
Feature-Caps				RFC 6809 [125]
feature-param	A4	*+g.3gpp.atcf="tel:+1-237-888-9999"*	Rel-11	
	A4	*+g.3gpp.cs2ps-srvcc="<sip:sti-sr@atcf.visited2.net>"*	Rel-11	
Feature-Caps	A5	not present		
Content-Length				RFC 3261 [15]
value		0		

Condition	Explanation
A1	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A2	Response for an non-emergency registration
A3	Response for an emergency registration
A4	Response if the UE provided the +g.3gpp.cs2ps-srvcc and +g.3gpp.cs2ps-srvcc-alerting feature-params in the REGISTER message
A5	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])

NOTE 1: The set of IMPUs shall be in accordance to annex E.3 independent of whether the UE has an ISIM on the UICC or not (i.e. when the UE has no ISIM SS shall use the same values as if the UE would have an ISIM; furthermore in this case the temporary public user id shall not be included in the set of IMPUs)

NOTE 2: any arbitrary (but valid) TEL URI

NOTE 3: According to TS 24.229 clause 5.1.1.1A and 5.1.6.2 [10] when the UE is using ISIM the emergency public user identity is the first public user identity in the list stored in the ISIM; when there is no ISIM it is the default public user id if the UE non-emergency registered with the IM CN and the temporary user id (derived from IMSI) in all other cases.

A.1.4 SUBSCRIBE for reg-event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *SUBSCRIBE* Public user identity used for subscription (NOTE 1) *SIP/2.0*		RFC 3261 [15]
Route route-param route-param	 A1 A2	order of the parameters in this header must be like in the respective rows <*sip:*SS P-CSCF address:protected server port of P-CSCF*;lr*>*, <sip:scscf.3gpp.org;lr*> <*sip:*SS P-CSCF address: unprotected server port of P-CSCF (optional)*;lr*>*, <sip:scscf.3gpp.org;lr*>		RFC 3261 [15]
Via sent-protocol sent-by via-branch	 A1 A2	 *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP IP address or FQDN and protected server port of the UE IP address or FQDN, port (optional) and not checked value starting with '*z9hG4bK'*		RFC 3261 [15]
From addr-spec tag		 Public user identity used for subscription (NOTE 1) must be present, value not checked but stored for later reference		RFC 3261 [15]
To addr-spec tag		 Public user identity used for subscription (NOTE 1) not present		RFC 3261 [15]
Contact addr-spec addr-spec addr-spec	 A1 A2 A4	 SIP URI with IP address or FQDN and protected server port of UE SIP URI with IP address or FQDN and unprotected server port of UE Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response		RFC 3261 [15] RFC 5627 [61]
Expires delta-seconds		 *600000*		RFC 3261 [15]
Security-Verify sec-mechanism	A1	 same value as Security-Server header sent by SS		RFC 3329 [21]
Security-Verify	A5	not present		
Require option-tag	A1	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Require	A5	not present		
Proxy-Require option-tag	A1	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Proxy-Require	A5	not present		
CSeq value method		 value not checked *SUBSCRIBE*		RFC 3261 [15]
Call-ID callid		 value not checked, but stored for later reference		RFC 3261 [15]
Max-Forwards value		 non-zero value		RFC 3261 [15]
P-Access-Network-Info access-net-spec access-net-spec 	A1,A5 A1 AND A6 A5 A7	 access network information and, if applicable, the cell ID access network information for Fixed Broadband and if applicable DSL Location Parameter access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	 Rel-15	RFC 7315 [132] RFC 7913 [154]
Accept media-range		(if present) *application/reginfo+xml*		RFC 3261 [15] RFC 3680 [22]
Event event-type		 *reg*		RFC 6665 [140] RFC 3680 [22]

Content-Length value		header shall be present if UE uses TCP to send this message and if there is a message-body length of request body, if such is present		RFC 3261 [15]

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	Void
A4	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A5	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])
A6	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A7	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

NOTE 1: According to TS 24.229 clause 5.1.1.3 the public user identity used for subscription is:
a) when the UE has an ISIM the default public user identity or the public user identity used for initial registration
b) when the UE does not have an ISIM the default public user identity

A.1.5 200 OK for SUBSCRIBE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *200* *OK*		RFC 3261 [15]
Via via-parm		 same value as received in SUBSCRIBE message		RFC 3261 [15]
To addr-spec tag		 same value as received in SUBSCRIBE message common to-tag (subscribe dialog)		RFC 3261 [15]
From addr-spec tag		 same value as received in SUBSCRIBE message same value as received in SUBSCRIBE message		RFC 3261 [15]
Call-ID callid		 same value as received in SUBSCRIBE message		RFC 3261 [15]
CSeq value		 same value as received in SUBSCRIBE message		RFC 3261 [15]
Contact addr-spec		 *<scscf.3gpp.org>*		RFC 3261 [15]
Expires delta-seconds		 *600000*		RFC 3261 [15]
Record-Route addr-spec uri-parameter	 A1 A2,A3	 SS P-CSCF address: protected server port of SS SS P-CSCF address: unprotected server port of SS (optional) *lr*		RFC 3261 [15]
Content-Length value		 *0*		RFC 3261 [15]

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])

NOTE1: All choices for applicable conditions are described for each header.

A.1.6 NOTIFY for reg-event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI	A1	same URI as used by the UE in the corresponding REGISTER message and protected server port of UE		
Request-URI	A2,A5	same URI as used by the UE in the corresponding REGISTER message and unprotected server port of UE		
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15]
via-parm1:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address and protected server port of SS		
	A2,A5	IP address and unprotected server port of SS (optional)		
via-branch		value starting with '*z9hG4bK'* (NOTE 3)		
via-parm2:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		*scscf.3gpp.org*		
via-branch		value starting with '*z9hG4bK'* (NOTE 3)		
From				RFC 3261 [15]
addr-spec		same URI as received in the To header of the previous SUBSCRIBE message (NOTE 2)		
tag		common to-tag (subscribe dialog)		
To				RFC 3261 [15]
addr-spec		same URI as received in the From header of the previous SUBSCRIBE message (NOTE 2)		
tag		same value as received in From tag of SUBSCRIBE message		
Call-ID				RFC 3261 [15]
callid		same as value received in SUBSCRIBE message		
CSeq	A1,A2,A5			RFC 3261 [15]
value		*1*		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec		*<sip:scscf.3gpp.org>*		
Content-Type				RFC 3261 [15]
media-type		*application/reginfo+xml*		RFC 3680 [22]
Event	A1,A2,A5			RFC 6665 [140]
event-type		*reg*		RFC 3680 [22]
Max-Forwards				RFC 3261 [15]
value		*69*		
Subscription-State				RFC 6665 [140]
substate-value		*active*		
expires		*600000*		
Content-Length				RFC 3261 [15]
value		length of message-body		

Header/param	Cond	Value/remark	Rel	Reference
Message-body	A3	<?xml version="1.0" encoding="UTF-8"?> <reginfo xmlns="urn:ietf:params:xml:ns:reginfo" version="0" state="full"> <registration aor="PublicUserIdentity1 (NOTE 1) " id="a100" state="active"> <contact id="980" state="active" event="registered"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor="AssociatedTelUri (NOTE 1) " id="a101" state="active"> <contact id="981" state="active" event="created"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor="PublicUserIdentity2 (NOTE 1) " id="a102" state="active"> <contact id="982" state="active" event="registered"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor="PublicUserIdentity3 (NOTE 1) " id="a103" state="active"> <contact id="983" state="active" event="registered"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> </reginfo>		RFC 3680 [22]

	A4	<?xml version="1.0" encoding="UTF-8"?> <reginfo xmlns="urn:ietf:params:xml:ns:reginfo" xmlns:gr="urn:ietf:params:xml:ns:gruuinfo" version="0" state="full"> <registration aor="PublicUserIdentity1 (NOTE 1) " id="a100" state="active"> <contact id="980" state="active" event="registered" callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> <gr:pub-gruu uri="public GRUU associated to this aor"/> <gr:temp-gruu uri="temporary GRUU associated to this aor" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> <registration aor="AssociatedTelUri (NOTE 1) " id="a101" state="active"> <contact id="981" state="active" event="created"><uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> <gr:pub-gruu uri=" same public GRUU as for PublicUserIdentity1"/> <gr:temp-gruu uri=" same temporary GRUU as for PublicUserIdentity1" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> <registration aor="PublicUserIdentity2 (NOTE 1) " id="a102" state="active"> <contact id="982" state="active" event="registered"callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> <gr:pub-gruu uri="public GRUU associated to this aor"/> <gr:temp-gruu uri="temporary GRUU associated to this aor" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> <registration aor="PublicUserIdentity3 (NOTE 1) " id="a103" state="active"> <contact id="983" state="active" event="registered"callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param>		RFC 5628 [62]

Header/param	Cond	Value/remark	Rel	Reference
		<gr:pub-gruu uri="public GRUU associated to this aor"/> <gr:temp-gruu uri="temporary GRUU associated to this aor" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> </reginfo>		
Message-body	A5	<?xml version="1.0" encoding="UTF-8"?> <reginfo xmlns="urn:ietf:params:xml:ns:reginfo" version="0" state="full"> <registration aor="PublicUserIdentity1 (NOTE 1) " id="a100" state="active"> <contact id="980" state="active" event="registered"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor="AssociatedTelUri (NOTE 1) " id="a101" state="active"> <contact id="981" state="active" event="created"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> </reginfo>		
Message-body	A3 AND A6	<?xml version="1.0" encoding="UTF-8"?> <reginfo xmlns="urn:ietf:params:xml:ns:reginfo" version="1" state="full"> <registration aor="PublicUserIdentity1 (NOTE 1)" id="a100" state="terminated"> <contact id="980" state="terminated" event="deactivated"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor="AssociatedTelUri (NOTE 1)" id="a101" state="terminated"> <contact id="981" state="terminated" event="deactivated"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor="PublicUserIdentity2 (NOTE 1)" id="a102" state="terminated"> <contact id="982" state="terminated" event="deactivated"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor="PublicUserIdentity3 (NOTE 1)" id="a103" state="terminated"> <contact id="983" state="terminated" event="deactivated"> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> </reginfo>		

Message-body	A4 AND A6	<?xml version="1.0" encoding="UTF-8"?> <reginfo xmlns="urn:ietf:params:xml:ns:reginfo" xmlns:gr="urn:ietf:params:xml:ns:gruuinfo" version="1" state="full"> <registration aor="PublicUserIdentity1 (NOTE 1)" id="a100" state="terminated"> <contact id="980" state="terminated" event="deactivated" callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance">"Instance ID of the UE;"</unknown-param> <gr:pub-gruu uri="public GRUU associated to this aor"/> <gr:temp-gruu uri="temporary GRUU associated to this aor" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> <registration aor="AssociatedTelUri (NOTE 1)" id="a101" state="terminated"> <contact id="981" state="terminated" event="deactivated" <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance">"Instance ID of the UE;" </unknown-param> <gr:pub-gruu uri="same public GRUU as for PublicUserIdentity1"/> <gr:temp-gruu uri="same temporary GRUU as for PublicUserIdentity1" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> <registration aor="PublicUserIdentity2 (NOTE 1)" id="a102" state="terminated"> <contact id="982" state="terminated" event="deactivated" callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance">"Instance ID of the UE;"</unknown-param> <gr:pub-gruu uri="public GRUU associated to this aor"/> <gr:temp-gruu uri="temporary GRUU associated to this aor" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration> <registration aor="PublicUserIdentity3 (NOTE 1)" id="a103" state="terminated"> <contact id="983" state="terminated" event="deactivated" callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <unknown-param name="+sip.instance">"Instance ID of the UE;" </unknown-param> <gr:pub-gruu uri="public GRUU associated to this aor"/> <gr:temp-gruu uri="temporary GRUU associated to this aor" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </contact> </registration>		

Header/param	Cond	Value/remark	Rel	Reference
		</reginfo>		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5]
A3	NOT obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A4	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A5	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])
A6	NOTIFY sent by SS for de-registering the UE

NOTE 1: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI;
AssociatedTelUri is the same as used in P-Associated-URI
PublicUserId2 and PublicUserId3 are the remaining IMPUs of the P-Associated-URI header

NOTE 2: This results in using the public user identity used for subscription as defined in TS 24.229 clause 5.1.1.3.

NOTE 3: Branch parameter values sent by SS are different within a test case execution.

A.1.7 423 Interval Too Brief for REGISTER

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*423*		
Reason-Phrase		*Interval Too Brief*		
Via				RFC 3261 [15]
via-parm		same value as received in REGISTER message		
To				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
tag		common to-tag (register)		
From				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
Call-ID				RFC 3261 [15]
callid		same value as received in REGISTER message		
CSeq				RFC 3261 [15]
value		same value as received in REGISTER message		
Min-Expires				RFC 3261 [15]
delta-seconds		T (a decimal integer number of seconds between 0 and (2**32)-1)		

A.1.8 420 Bad Extension for REGISTER

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*420*		
Reason-Phrase		*Bad Extension*		
Via				RFC 3261 [15]
via-parm		same value as received in REGISTER message		
To				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
tag		common to-tag (register)		
From				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
Call-ID				RFC 3261 [15]
callid		same value as received in REGISTER message		
CSeq				RFC 3261 [15]
value		same value as received in REGISTER message		
Unsupported				RFC 3261 [15]
option-tag		*sec-agree*		
Content-Type	A1			RFC 3261 [15]
media-type		*application/3gpp-ims+xml*		
Message-body	A1	*<?xml version="1.0" encoding="UTF-8"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>emergency</type>* *<action>anonymous-emergencycall</action>* *<reason></reason>* *</alternative-service>* *</ims-3gpp>* (see NOTE 1)		

Condition	Explanation
A1	IMS emergency call for an anonymous emergency call

NOTE 1: This XML body is defined in Rel-14 TS 24.229 [10] and may be ignored by pre-Rel-14 UE.

A.2 Default messages for Call Setup

A.2.1 INVITE for MO Call Setup

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				
Method		*INVITE*		RFC 3261 [15]
Request-URI	NOT A5	px_IMS_CalleeUri px_IMS_CalleeURI may be either SIP or Tel URI. It may contain a dialstring and phone-context parameter, when calling to dialstring. When calling to dialstring SIP URI must also contain user=phone or user=dialstring parameter. The dialstring, if used, may be global, home local number or geo-local number. For home local numbers the value of phone-context parameter must equal the home domain name i.e. px_IMS_HomeDomainName. For geo-local numbers the home domain name must be prefixed by string "geo-local." or access technology specific prefix, if the UE supports that option. Note: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is UE implementation specific. For instance the UE might have a UI setting		TS 24.229 [10] cl 5.1.2A.1.3, 5.1.2A.1.5, 7.2A.10
	A5	px_IMS_CalleeContactUri		
	A6,A7	emergency service URN beginning with *urn:service:sos*		RFC 5031 [97]
	A20 AND (NOT A25)	*urn:service:sos.ecall.manual*	Rel-14	RFC 8147 [149]
	A21 AND (NOT A25)	*urn:service:sos:ecall.automatic*	Rel-14	RFC 8147 [149]
	A25	The Test URI as per the generic "eCall test URI" which uses EF_{SDNURI} from table 4.9.3.5-1 for "eCall capable" UEs or EF_{FDNURI} from table 4.9.3.5-2 for "eCall only" UEs as specified in 3GPP TS 36.508 [94]	Rel-14	RFC 8147 [149]
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1,A7	IP address or FQDN and protected server port of the UE		
	A2,A19	IP address or FQDN, port (optional) and not checked		
	A6	IP address and, when using UDP, unprotected server port of the UE		
	A17	IP address and unprotected server port of the UE		
response-port	A6	*rport* (when using UDP)		RFC 3581 [96]
via-branch		value starting with '*z9hG4bK'*		
Route		order of the parameters in this header must be like in the respective rows		RFC 3261 [15]
route-param	A1	<*sip:*SS P-CSCF address: protected server port of SS*;lr>, <sip:scscf.3gpp.org;lr>*		
	A2,A17	<*sip:*SS P-CSCF address: unprotected server port of SS (optional)*;lr>, <sip:scscf.3gpp.org*f*;lr*		
	A5	MO call has been established: URIs of the Record-Route header of 183 response in reverse order (or any other response creating the dialog according to RFC 3261 clause 12.1 [15]) MT call has been established: same value as defined for the Record-Route header in A.2.9		
	A6,A19	<*sip:*SS P-CSCF address: unprotected server port of SS*;lr>*		
	A7	<*sip:*SS P-CSCF address: protected server port of SS*;lr>*		
From				RFC 3261 [15]
addr-spec	A6	Any SIP URI with display name as "*Anonymous"* or anonymous		
	A7,A19	emergency public user identity (NOTE 3)		

	A4	any SIP URI being subscribed and registered as listed in the XML body of the NOTIFY request; additionally when there is a P-Preferred-Identity header within the INVITE request the SIP URI shall match the URI within the P-Preferred-Identity header		
tag	A4	must be present, value not checked		
addr-spec	A5	local SIP URI of the UE as used in any previous request in the same dialog (In the earlier requests within the same dialog this URI appears in From header within requests sent by the UE and in To header within requests sent by the SS)		
tag	A5	local tag of the dialog ID (In the earlier requests within the same dialog this tag appears in From header within requests sent by the UE and in To header within requests sent by the SS)		
To				RFC 3261 [15]
addr-spec	A6,A7	emergency service URN beginning as *urn:service:sos*		RFC 5031 [97]
	A20 AND (NOT A25)	*urn:service:sos.ecall.manual*	Rel-14	RFC 8147 [149]
	A21 AND (NOT A25)	*urn:service:sos:ecall:automatic*	Rel-14	RFC 8147 [149]
	A25	The Test URI as per the generic "eCall test URI" which uses EF_{SDNURI} from table 4.9.3.5-1 for "eCall capable" UEs or EF_{FDNURI} from table 4.9.3.5-2 for "eCall only" UEs as specified in 3GPP TS 36.508 [94]	Rel-14	RFC 8147 [149]
	A4	px_IMS_CalleeUri		
tag	A4	not present		
addr-spec	A5	remote SIP URI of SS (i.e. the remote UE) as used in any previous request in the same dialog (In the earlier requests within the same dialog this URI appears in To header within requests sent by the UE and in From header within requests sent by the SS)		
tag	A5	remote tag of the dialog ID (In the earlier requests within the same dialog this tag appears in To header within requests sent by the UE and in From header within requests sent by the SS)		
Call-ID				RFC 3261 [15]
callid	A4	value different to that received in REGISTER message		
	A5	value of Call-ID as in any previous request in the same dialog		
Call-Info	A20,A21		Rel-14	RFC 8147 [149]
cid URL		any URL		
purpose		*emergencyCallData.eCall.MSD*		
CSeq				RFC 3261 [15]
value	A4	must be present, value not checked		
	A5	value of CSeq sent by the UE within its previous request in the same dialog but increased by one		
method		*INVITE*		
Supported		The option tags defined below shall be included additionally to any option tags defined in any specific message content, unless specified otherwise in this specific message content.		RFC 3261 [15]
option-tag		*100rel*		
	A13 OR A14	*norefersub*	Rel-11	RFC 4488 [126]
	A4 AND A26 AND NOT (A6 OR A7 OR A19 OR A20 OR A21)	*timer*		RFC 4028 [146]
P-Early-Media	A16 AND (NOT A5)			RFC 5009 [138] IR.92 [133]
em-param		*supported*		
Geolocation	A8		Rel-9	RFC 6442 [98]

locationURI		cid-url indicating the Content-Id of the PIDF-LO within the multipart MIME body of INVITE request. (Note that location-by-reference URI is not allowed as the SS does not provide any external storage for location info for the UE to refer.)		
Geolocation-Routing	A8	"yes"	Rel-9	RFC 6442 [98]
Require option-tag	A1,A7 A6 A1,A7	 not present *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Proxy-Require option-tag	A1,A7 A6 A1,A7	 not present *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Security-Verify sec-mechanism	A1,A7 A2,A6 A1,A7	 not present same value as Security-Server header sent by SS		RFC 3329 [21]
Contact addr-spec	 (A1 OR A7) AND NOT A15 (A2 OR A19) AND NOT A15 A15 AND NOT A6 A6	 SIP URI with IP address or FQDN and protected server port of UE SIP URI with IP address or FQDN and unprotected server port of UE Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response SIP URI with IP address and unprotected server port of UE		RFC 3261 [15] RFC 5627 [61]
c-p-instance	A6 A3,A17	*+sip.instance="<urn:gsma:imei*: (gsma-specifier-defined-substring)>" where gsma-specifier-defined-substring shall be the IMEI code of the UE, coded as specified in RFC 7254 [122], without optional parameters *+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"* (see NOTE 2, 4)	Rel-10	RFC 5626 [109] RFC 7254 [122]
feature-param	A10 A12 A22 AND (A23 OR A24) A18 AND NOT A5	*video* *+g.3gpp.srvcc-alerting* *audio* *+g.3gpp.ps2cs-srvcc-orig-pre-alerting*		RFC 3840 [63] RFC 3840 [63] RFC 3840 [63] RFC 3840 [63]
Max-Forwards value		 non-zero value		RFC 3261 [15]
P-Access-Network-Info access-net-spec	NOT A2 A1 AND A27 A28	 access network information and, if applicable, the cell ID access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	 Rel-15	RFC 7315 [132] RFC 7913 [154]
P-Access-Network-Info access-net-spec	A2(o)	header optional access network information and, if applicable, the cell ID		
Accept media-range	NOT A5 A5(o) A4 A13 A14 A20,A21	 header optional *application/sdp,application/3gpp-ims+xml* (additional medias can be added in any order) *application/vnd.3gpp.mid-call+xml* *application/vnd.3gpp.state-and-event-info+xml* *application/EmergencyCallData.Control+xml*	Rel-7 Rel-11 Rel-11 Rel-14	RFC 3261 [15] RFC 8147 [149]
P-Preferred-Service Service-ID	 A3 AND A4	 *urn:urn-7:3gpp-service.ims.icsi.mmtel*		RFC 6050 [68]

P-Preferred-Identity PPreferredID-value	 A7	 emergency public user identity (NOTE 3)		RFC 3325 [89]
Recv-Info Info-package-type	 A14 A20,A21	 *g.3gpp.state-and-event* *EmergencyCallData.eCall.MSD*	 Rel-14	RFC 6086 [139] RFC 8147 [149]
Accept-Contact ac-value	 A3 AND A4 A10 AND A11	 *+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"* (see NOTE 2, 4) *video*		RFC 3841 [64]
Proxy-Authorization username realm nonce digest-uri qop-value cnonce-value nonce-count response algorithm	A17 A17 A17 A17 A17 A17 A17 A17 A17 A17	 preconfigured in the UE same value as received in the realm directive in the Proxy-Authorization header sent by SS same value as in Proxy-Authorization header sent by SS preconfigured in the UE *auth* value assigned by UE affecting the response calculation counter to indicate how many times UE has sent the same value of nonce within successive INVITESs, initial value shall be 1 response calculated by UE *MD5*		RFC 2617 [16] RFC 3310 [17]
Content-Type media-type	 NOT A8 AND NOT A20 AND NOT A21 AND NOT A25 A8,A20,A21 A25	 *application/sdp* *multipart/mixed;boundary=*any value		RFC 3261 [15] RFC 6442 [98] RFC 8147 [149]
Content-Length Value		header shall be present if UE uses TCP to send this message and if there is a message body length of message-body		RFC 3261 [15]
Message-body	 A8 (A20 OR A21) AND NOT A25	consists of one or several parts as indicated by Content-Type, and each part having actual contents as follows (SDP contents, if any, is specified in dedicated sections) a PIDF-LO element mapped to the same Content-ID which can be found from the Geolocation header The PIDF-LO shall contain at least the following elements: - One or more 'geopriv' elements, each containing: - One 'location-info' element describing the location of the UE; and - One 'usage-rules' element describing the limitations of the usage of the location info --boundary value (as provided in SIP hdr Content-Type) *Content-Type: application/EmergencyCallData.eCall.MSD* *Content-ID:* same URL as in Call-Info header *Content-Disposition: by-reference;handling=optional* MSD in ASN.1 PER encoding --boundary value (as provided in SIP hdr Content-Type)	 Rel-14	 RFC 8147 [149]

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	UE supports MTSI (A.3A/50 3GPP TS 34.229-2 [5])
A4	INVITE creating a dialog
A5	re-INVITE within a dialog

A6	INVITE for creating an emergency session in case of no registration
A7	INVITE for creating an emergency session within an emergency registration using IMS security
A8	UE is capable of obtaining location information, has obtained its location and is setting up an emergency session
A9	Void
A10	UE supports video feature tag (A.12/32 3GPP TS 34.229-2 [5])
A11	INVITE for creating a video call
A12	INVITE for creating a voice or video call and UE supports g.3gpp.srvcc-alerting media feature tag (A.12/34 3GPP TS 34.229-2 [5])
A13	INVITE for creating a voice call during rSRVCC and UE CS to PS SRVCC with the MSC assisted mid-call feature (A.12/42 3GPP TS 34.229-2 [5])
A14	INVITE for creating a voice call and UE supports CS to PS SRVCC for calls in alerting phase (A.12/41 3GPP TS 34.229-2 [5])
A15	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A16	UE supports early media (A.12/45 3GPP TS 34.229-2 [5])
A17	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])
A18	UE indicates g.3gpp.ps2cs-srvcc-orig-pre-alerting media feature tag in INVITE request (A.12/36 3GPP TS 34.229-2 [5])
A19	INVITE for creating an emergency session within an emergency registration using GIBA
A20	INVITE for creating an eCall over IMS session manually
A21	INVITE for creating an eCall over IMS session automatically
A22	UE supports audio media feature tag (A.12/56 3GPP TS 34.229-2 [5])
A23	UE uses E-UTRAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.301 [150], clauses 8.2.1 and 9.9.3.12A
A24	UE uses UTRAN/GERAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.008 [12], clauses 9.4.2 and 10.5.5.23
A25	INVITE for creating a test eCall over IMS session
A26	UE supports Session Timer (A.12/57 3GPP TS 34.229-2 [5])
A27	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A28	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

NOTE 1: All choices for applicable conditions are described for each header.

NOTE 2: The “=” may include optional linear white spaces according to the EQUAL definition in chapter 25.1, RFC 3261 [15].

NOTE 3: According to TS 24.229 clause 5.1.1.1A and 5.1.6.2 [10] when the UE is using ISIM the emergency public user identity is the first public user identity in the list stored in the ISIM; when there is no ISIM it is the default public user id if the UE registered or the temporary user id (derived from IMSI) else.

NOTE 4: URN is the outcome of URL encoding (“Percent-Encoding” according to RFC 3986 [129]) of urn:urn-7:3gpp-service.ims.icsi.mmtel.

A.2.2 100 Trying for INVITE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*100*		
Reason-Phrase		*Trying*		
Via				RFC 3261 [15]
via-parm		same value as received in INVITE message		
From				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		same value as received in INVITE message		
To				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag	A1	not present		
tag	A2	may be present, not checked		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		same value as received in INVITE message		
Content-Length	A1			RFC 3261 [15]
value		*0*		

Condition	Explanation
A1	100 Trying sent from SS
A2	100 Trying sent from UE

A.2.3 183 Session Progress for INVITE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*183*		
Reason-Phrase		*Session Progress*		
Record-Route		order of the parameters in this header must be like in the respective rows		RFC 3261 [15]
rec-route	A1	<*sip:pcscf.other.com;lr*>, <*sip:scscf.other.com*;*lr*>, <*sip:orig@scscf.3gpp.org*;*lr*>, <*sip*:SS P-CSCF address: protected server port of SS;*lr*>		
	A3	<*sip:pcscf.other.com*;*lr*>, <*sip:scscf.other.com*;*lr*>, <*sip:orig@scscf.3gpp.org*;*lr*>, <sip:SS P-CSCF address: unprotected server port of SS (optional);*lr*>		
	A2	same value as received in INVITE		
	A4	same value as received in INVITE		
	A5	<*sip:orig@ecscf.other.com;lr*>*,* <*sip:*SS P-CSCF address:protected server port of SS*;lr*>		
Via				RFC 3261 [15]
via-parm		same value as received in INVITE message		
Require		The option tags defined below shall be included additionally to any option tags defined in any specific message content, unless specified otherwise in this specific message content.		RFC 3261 [15]
option-tag		*100rel*		
From				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		same value as received in INVITE message		
To				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag	A1,A3, A5,A6	common to-tag (invite)		
	A2,A4	any value		
P-Asserted-Identity	A5			RFC 3325 [89]
addr-spec		A tel URI that can be recognized as valid emergency numbers if dialled by the user are specified in 3GPP TS 22.101 [39]. The emergency numbers 112 and 911 are stored on the ME, in accordance with 3GPP TS 22.101 [39]		
uri-parameter		*lr*		
Contact				RFC 3261 [15]
addr-spec	A1,A3	px_IMS_CalleeContactUri		
	A2 AND NOT A9	SIP URI with IP address or FQDN and protected server port of UE		
	A4 AND NOT A9	SIP URI with IP address or FQDN and unprotected server port of UE		
	A2 AND A9	Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response		RFC 5627 [61]
	A4 AND A9	Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response		RFC 5627 [61]
feature-param		*+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"*(see NOTE 2, 3)		
	A6	*video*		
	A10	*audio*		
	A11 AND A12 AND (A13 OR A14)	*audio*		
RSeq				RFC 3262 [33]
response-num	A2,A4	any value		
	A1,A3	*121* (arbitrarily selected)		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		same value as received in INVITE message		
Feature-Caps				RFC 6809 [125]
feature-param	A8	*+g.3gpp.ps2cs-srvcc-orig-pre-alerting*		TS 24.237 [110]

Content-Type media-type		 *application/sdp*		RFC 3261 [15]
Content-Length value	A1,A3	 length of message-body		RFC 3261 [15]

Condition	Explanation
A1	183 sent by the SS (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A2	183 sent by the UE (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A3	183 sent by the SS (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A4	183 sent by the UE (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A5	183 sent by the SS for INVITE for a non-UE detectable emergency call
A6	UE supports video media feature tag (A.12/32 3GPP TS 34.229-2 [5])
A7	Void
A8	183 sent by the SS for a voice call and UE supports pre-alerting media feature tag (A.12/36 3GPP TS 34.229-2 [5])
A9	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A10	Void
A11	Void
A12	UE supports audio media feature tag (A.12/56 3GPP TS 34.229-2 [5])
A13	UE uses E-UTRAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.301 [150], clauses 8.2.1 and 9.9.3.12A.
A14	UE uses UTRAN/GERAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.008 [12], clauses 9.4.2 and 10.5.5.23.

NOTE1: All choices for applicable conditions are described for each header.

NOTE 2: The "=" may include optional linear white spaces according to the EQUAL definition in chapter 25.1, RFC 3261 [15].

NOTE 3: URN is the outcome of the URL encoding ("Percent-Encoding" according to RFC 3986 [129]) of urn:urn-7:3gpp-service.ims.icsi.mmtel.

A.2.4 PRACK

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*PRACK*		
Request-URI		same URI value as the recipient of PRACK has earlier sent in its Contact header within the same dialog		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by		same value as in preceding INVITE message		
via-branch		value starting with '*z9hG4bK'* (NOTE 1)		
Route	A1,A2			RFC 3261 [15]
route-param	A1,A2	URIs of the Record-Route header of 183 response (or 180 when applicable) in reverse order		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE when PRACK is sent by the UE, but SIP URI of the SS when PRACK is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		local tag of the dialog ID		
To				RFC 3261 [15]
addr-spec		SIP URI of the SS when PRACK is sent by the UE, but SIP URI of the UE when PRACK is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		remote tag of the dialog ID		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one		
method		*PRACK*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
RAck				RFC 3262 [33]
response-num		same value as in RSeq header of the reliable response		
cseq-num		same value as in CSeq of the reliable response		
method		same value as in CSeq of the reliable response		
P-Access-Network-Info	A1,A2(o)			RFC 7315 [132] RFC 7913 [154]
access-net-spec	A6	access network information and, if applicable, the cell ID		
	A7	access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	Rel-15	
Proxy-Authorization	A5			RFC 2617 [16] RFC 3310 [17]
username	A5	preconfigured in the UE		
realm	A5	same value as received in the realm directive in the Proxy-Authorization header sent by SS		
nonce	A5	same value as in Proxy-Authorization header sent by SS		
digest-uri	A5	preconfigured in the UE		
qop-value	A5	*auth*		
cnonce-value	A5	value assigned by UE affecting the response calculation		
nonce-count	A5	counter to indicate how many times UE has sent the same value of nonce within successive INVITEs, initial value shall be 1		
response	A5	response calculated by UE		
algorithm	A5	*MD5*		
Content-Type		header shall be present only if there is SDP in Message-body		RFC 3261 [15]
media-type		*application/sdp*		
Content-Length				RFC 3261 [15]
value		length of Message-body		
Message-body		Optional SDP body. If included then the contents of the SDP shall be checked as described in the Test requirements section of the test case.		RFC 4566 [27] RFC 3264 [30] RFC 3312 [31]

Condition	Explanation
A1	PRACK sent by the UE (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A2	PRACK sent by the UE (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A3	PRACK sent by the SS (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A4	PRACK sent by the SS (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A5	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])
A6	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A7	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.2.5 UPDATE

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *UPDATE* same URI value as the recipient of UPDATE has earlier sent in its Contact header within the same dialog *SIP/2.0*		RFC 3261 [15]
Via sent-protocol sent-by via-branch	 A1,A2 A3,A4	 *SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP) MO call: same value as in INVITE message MT call: as defined in A.2.1 as defined in A.2.9 (There is more than one value) value starting with '*z9hG4bK'* (NOTE 2)		RFC 3261 [15]
Route route-param	A1,A2	 URIs of the Record-Route header of 183 response in reverse order		RFC 3261 [15]
From addr-spec tag		 SIP URI of the UE when UPDATE is sent by the UE, but SIP URI of the SS when UPDATE is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog. local tag of the dialog ID		 RFC 3261 [15]
To addr-spec tag		 SIP URI of the SS when UPDATE is sent by the UE, but SIP URI of the UE when UPDATE is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog. remote tag of the dialog ID		RFC 3261 [15]
Call-ID callid		 same value as received in INVITE message		RFC 3261 [15]
Contact	A1,A2 A3,A4	Must be present, value not checked MO call: same Contact header as sent by SS in this dialog (e.g. in a 183 or 180 response) MT call: same value as used in MT INVITE		RFC 3261 [15] RFC 3311 [137]
CSeq value method		 value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one *UPDATE*		RFC 3261 [15]
Require option-tag	A1 A1	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Proxy-Require option-tag	A1 A1	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Max-Forwards value		 non-zero value		RFC 3261 [15]
Security-Verify sec-mechanism	A1	 same value as Security-Server header sent by SS		RFC 3329 [21]
Security-Verify sec-mechanism	A2	not present		RFC 3329 [21]
P-Access-Network-Info access-net-spec	A1,A2(o) A5 A6	 access network information and, if applicable, the cell ID access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	 Rel-15	RFC 7315 [132] RFC 7913 [154]
Content-Type media-type		 *application/sdp*		RFC 3261 [15]
Content-Length	A3,A4			RFC 3261 [15]

value		length of message-body		
Message-body		Contents of the SDP body shall be checked as described in the Test requirements section of the test case.		RFC 4566 [27] RFC 3264 [30] RFC 3312 [31]

Condition	Explanation
A1	UPDATE sent by the UE (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A2	UPDATE sent by the UE (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A3	UPDATE sent by the SS (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A4	UPDATE sent by the SS (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A5	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A6	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

NOTE 1: All choices for applicable conditions are described for each header.

NOTE 2: Branch parameter values sent by SS are different within a test case execution.

A.2.6 180 Ringing for INVITE

Header/param	Cond	Value/remark	Rel	Reference
Request-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *180* *Ringing*		RFC 3261 [15]
Record-Route rec-route	 A7 A8	 as defined for the common 183 response, see A.2.3 <*sip:orig@ecscf.other.com;lr*>, <*sip:*SS P-CSCF address:unprotected server port of SS*;lr*> <*sip:orig@ecscf.other.com;lr*>, <*sip:*SS P-CSCF address:protected server port of SS*;lr*>		RFC 3261 [15]
Via via-parm		 same value as received in INVITE message		RFC 3261 [15]
Require option-tag	 A3	The option tags defined below shall be included additionally to any option tags defined in any specific message content, unless specified otherwise in this specific message content. *100rel*		RFC 3261 [15]
From addr-spec tag		 same value as received in INVITE message same value as received in INVITE message		RFC 3261 [15]
To addr-spec tag		 same value as received in INVITE message as defined for the common 183 response, see A.2.3		RFC 3261 [15]
P-Asserted-Identity addr-spec uri-parameter	A4	 A tel URI that can be recognized as valid emergency numbers if dialled by the user are specified in 3GPP TS 22.101 [39]. The emergency numbers 112 and 911 are stored on the ME, in accordance with 3GPP TS 22.101 [39] *lr*		RFC 3325 [89]
Contact addr-spec feature-param	 A5 A1 A2 AND A9 AND (A10 OR A11)	 as defined for the common 183 response, see A.2.3 *+g.3gpp.srvcc-alerting* *audio* *audio*		RFC 3261 [15]
RSeq response-num	 A3 AND NOT A12 A1 AND A12 A2 AND A12	 previous RSeq number sent in the same direction incremented by one *122* any value		RFC 3262 [33]
Call-ID callid		 same value as received in INVITE message		RFC 3261 [15]
CSeq value		 same value as received in INVITE message		RFC 3261 [15]
P-Access-Network-Info access-net-spec	A2 A13 A14	 access network information and, if applicable, the cell ID access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	 Rel-15	RFC 7315 [132] RFC 7913 [154]
P-Access-Network-Info	A1	not present		
Feature-Caps feature-param	 A6	 *+g.3gpp.srvcc-alerting*		
Content-Length value	A1	 length of message-body		RFC 3261 [15]

Condition	Explanation
A1	180 sent by the SS
A2	180 sent by the UE
A3	Response sent reliably (e.g. always when it contains an SDP body)
A4	180 sent by the SS when setting up an emergency call or a non-UE detectable emergency call
A5	180 sent by the UE for a voice or video call and UE supports g.3gpp.srvcc-alerting media feature tag (A.12/34 3GPP TS 34.229-2 [5])
A6	180 sent by the SS for a voice or video call and UE supports g.3gpp.srvcc-alerting media feature tag (A.12/34 3GPP TS 34.229-2 [5])
A7	Response sent by SS for emergency call without emergency registration
A8	Response sent by SS for emergency call with emergency registration or a non-UE detectable emergency call
A9	UE supports audio media feature tag (A.12/56 3GPP TS 34.229-2 [5])
A10	UE uses E-UTRAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.301 [150], clauses 8.2.1 and 9.9.3.12A.
A11	UE uses UTRAN/GERAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.008 [12], clauses 9.4.2 and 10.5.5.23.
A12	180 Ringing is first provisional response sent reliably in this dialog
A13	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A14	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

A.2.7 ACK

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*ACK*		
Request-URI	NOT A4	same URI value as the recipient of ACK sent earlier in its Contact header within the same dialog		
	A4	same value as in INVITE message		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol	A1	*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
	A2	same value as in INVITE message		
sent-by		same value as in INVITE message		
via-branch	A3	value starting with *'z9hG4bk'*		
	A4	same value as received in INVITE		
Route				RFC 3261 [15]
route-param	A1 AND A3 AND (NOT A5)	URIs of the Record-Route header sent to the UE in 183, 180 or 200 response (whichever response used for INVITE to be acknowledged and contained Record-Route header) in reverse order		
	A1 AND A4 AND (NOT A5)	Contents shall be the same as Route header sent in INVITE		
	A1 AND A5	Contents shall be the same as Route header in re-INVITE		
From				RFC 3261 [15]
addr-spec	A1	SIP URI of the UE as received in INVITE.		
	A2	SIP URI of the SS as sent in INVITE		
tag		local tag of the dialog ID (same as from-tag in the INVITE message)		
To				RFC 3261 [15]
addr-spec	A1	SIP URI of the SS as received in INVITE.		
	A2	SIP URI of the UE as sent in INVITE		
tag		remote tag of the dialog ID (as chosen in an earlier response of the dialog)		
Call-ID				RFC 3261 [15]
callid		same value as in INVITE message		
CSeq				RFC 3261 [15]
value		same value as in INVITE message		
method		*ACK*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Content-Length	A2			RFC 3261 [15]
value		*0*		

Condition	Explanation
A1	ACK sent by the UE
A2	ACK sent by the SS
A3	ACK for 2xx response
A4	ACK for non-2xx response
A5	ACK for re-INVITE

A.2.8 BYE

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *BYE* same URI value as the recipient of BYE has earlier sent in its Contact header within the same dialog *SIP/2.0*		RFC 3261 [15]
Via sent-protocol sent-by via-branch	 A1,A2 A3,A4	 *SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP) MO Call has been established: same value as in INVITE message MT Call has been established: as defined in A.2.1 as defined in A.2.9 **(There is more than one value)** value starting with '*z9hG4bK'* (NOTE 1)		RFC 3261 [15]
Route route-param	 A1,A2	 MO Call has been established: URIs of the Record-Route header of 183 response in reverse order (or any other response creating the dialog according to RFC 3261 clause 12.1 [15]) MT Call has been established: value of Record-Route header as defined in A.2.9		RFC 3261 [15]
Route	A3,A4	not present		
From addr-spec tag		 SIP URI of the UE when BYE is sent by the UE. SIP URI of the SS when BYE is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog. local tag of the dialog ID		RFC 3261 [15]
To addr-spec tag		 SIP URI of the SS when BYE is sent by the UE. SIP URI of the UE when BYE is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog. remote tag of the dialog ID		RFC 3261 [15]
Call-ID callid		 same value as sent or received in INVITE message		RFC 3261 [15]
CSeq value method		 value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one *BYE*		RFC 3261 [15]
Require option-tag	(A1 OR A5) AND NOT A6 A1,A5	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Require	A2, A6	not present		
Proxy-Require option-tag	(A1 OR A5) AND NOT A6 A1,A5	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Proxy-Require	A2,A6	not present		
Security-Verify sec-mechanism	(A1 OR A5) AND NOT A6 A1,A5	 same value as Security-Server header sent by SS		RFC 3329 [21]
Security-Verify	A2,A6	not present		
Max-Forwards value		 non-zero value		RFC 3261 [15]
P-Access-Network-Info access-net-spec	A1,A2(o) A7 A8	 access network information and, if applicable, the cell ID access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	 Rel-15	RFC 7315 [132] RFC 7913 [154]

Proxy-Authorization	A5			RFC 2617 [16] RFC 3310 [17]
username	A5	preconfigured in the UE		
realm	A5	same value as received in the realm directive in the Proxy-Authorization header sent by SS		
nonce	A5	same value as in Proxy-Authorization header sent by SS		
digest-uri	A5	preconfigured in the UE		
qop-value	A5	*auth*		
cnonce-value	A5	value assigned by UE affecting the response calculation		
nonce-count	A5	counter to indicate how many times UE has sent the same value of nonce within successive INVITESs, initial value shall be 1		
response	A5	response calculated by UE		
algorithm	A5	*MD5*		
Content-Length	A3,A4			RFC 3261 [15]
value		length of message body		

Condition	Explanation
A1	BYE sent by the UE (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A2	BYE sent by the UE (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A3	BYE sent by the SS (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A4	BYE sent by the SS (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A5	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])
A6	BYE for emergency call with no registration
A7	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A8	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.2.9 INVITE for MT Call

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version	 A4 A5 A10	 *INVITE* UE's registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message UE's contact address in SIP URI form, as provided in the Contact header within any response or request within the dialog UE's registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message with the tag *user = phone* *SIP/2.0*		RFC 3261 [15]
Via sent-protocol sent-by via-branch	 A1 A2	 *SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP) The SS P-CSCF address and the SS protected server port The SS P-CSCF address and the SS unprotected server port (optional) Value starting with '*z9hG4bK'*		RFC 3261 [15]
Via via-parm		In addition to the via-parm entry for the SS, the following via-parm entries are included: *SIP/2.0/UDP scscf1.3gpp.org;branch=z9hG4bK…,* *SIP/2.0/UDP scscf2.3gpp.org;branch=z9hG4bK...,* *SIP/2.0/UDP pcscf2.3gpp.org;branch=z9hG4bK...,* *SIP/2.0/UDP caller.3gpp.org:6543;branch=z9hG4bK...* (NOTE 2)		RFC 3261 [15]
Record-Route rec-route	 A1 AND A4 A2 AND A4	 <sip: SS P-CSCF address: protected server port of SS ;lr> <sip: SS P-CSCF address: unprotected server port of SS (optional);lr>		RFC 3261 [15]
Record-Route rec-route		In addition to the rec-route entry for the SS, the following rec-route entries are included: *<sip:term@scscf1.3gpp.org;lr>, <sip:orig@scscf2.3gpp.org;lr>, <sip:pcscf2.3gpp.org;lr>*		RFC 3261 [15]
Record-Route rec-route	 A1 AND A5	 MO call established: same value as in 183 Session Progress for INVITE, condition A1, in reverse order MT call established: <sip: SS P-CSCF address: protected server port of SS ;lr>		RFC 3261 [15]
Record-Route rec-route	 A2 AND A5	 MO call established: same value as in 183 Session Progress for INVITE, condition A3, in reverse order MT call established: <sip: SS P-CSCF address: unprotected server port of SS (optional);lr>		RFC 3261 [15]
From addr-spec tag addr-spec tag	 A4 A4 A5 A5	 SIP URI of the SS representing the calling UE any value SIP URI of the SS representing the calling UE as used in any previous request in the same dialog (In the earlier requests within the same dialog this URI appears in To header within requests sent by the UE and in From header within requests sent by the SS) local tag of the dialog ID		RFC 3261 [15]
To addr-spec tag addr-spec	 A4 A4 A5	 SIP URI of the UE's default public user id not present SIP URI of the UE as used in any previous request in the same dialog (In the earlier requests within the same dialog this URI appears in From header within requests sent by the UE and in To header within requests sent by the SS)		RFC 3261 [15]

tag	A5	remote tag of the dialog ID		
Call-ID callid	 A4 A5	 a random text string generated by the SS value of Call-ID as in any previous request in the same dialog		RFC 3261 [15]
CSeq value method	 A4 A5	 any value (e.g. 4711) value of CSeq sent by the SS within its previous request in the same dialog but increased by one *INVITE*		RFC 3261 [15]
Supported option-tag		The option tags defined below shall be included additionally to any option tags defined in any specific message content, unless specified otherwise in this specific message content. *100rel* *timer*		RFC 3261 [15] RFC 4028 [146]
P-Called-Party-ID		One of the UE's registered, non-barred public ID		RFC 7315 [132]
Contact addr-spec feature-param	 A1 A2 A5 A3 A7	 SIP URI with IP address or FQDN and protected server port of the calling UE, for example "sip:caller@3gpp.org:6543" SIP URI with IP address or FQDN and unprotected server port of the calling UE same contact information for the SS as used before in this dialog *+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"* (NOTE 1) *video* *audio*		RFC 3261 [15]
Feature-Caps feature-param	 A9	 *g.3gpp.srvcc-alerting*		
Max-Forwards value		 non-zero value		RFC 3261 [15]
Accept media-range	 A4	 *application/sdp, application/3gpp-ims+xml*	Rel-7	RFC 3261 [15]
P-Asserted-Service Service-ID	 A3 AND A4	 *urn:urn-7:3gpp-service.ims.icsi.mmtel*		RFC 6050 [68]
Accept-Contact ac-value ac-value	 A3 AND A4 A8	 **;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"* (NOTE 1) *video*		RFC 3841 [64]
Content-Type				RFC 3261 [15]
media-type		*application/sdp*		
Content-Length value		 length of message-body		RFC 3261 [15]

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	UE supports MTSI (A.3A/50 3GPP TS 34.229-2 [5])
A4	INVITE creating a dialog
A5	re-INVITE within a dialog
A6	Void
A7	UE supports video feature tag (A.12/32 3GPP TS 34.229-2 [5])
A8	INVITE for creating a video call and UE supports video media feature tag (A.12/32 3GPP TS 34.229-2 [5])
A9	INVITE for creating a voice or video call and UE supports g.3gpp.srvcc-alerting media feature tag (A.12/34 3GPP TS 34.229-2 [5])
A10	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])

NOTE 1: URN is the outcome of the URL encoding ("Percent-Encoding" according to RFC 3986 [129]) of urn:urn-7:3gpp-service.ims.icsi.mmtel.

NOTE 2: Branch parameter values sent by SS are different within a test case execution.

A.2.10 MO REFER

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*REFER*		
Request-URI		same URI value as the SS has earlier sent in its Contact header within the same dialog		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1	IP address or FQDN and protected server port of the UE		
	A2	IP address or FQDN and unprotected server port of the UE		
via-branch		value starting with '*z9hG4bK*'		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
route-param	A1	URIs of the Record-Route header of 183 response in reverse order		
	A2	URIs of the Record-Route header of 183 response in reverse order		
From				RFC 3261 [15]
addr-spec		local SIP URI of the UE which must be the same URI as used for the UE in the earlier requests within the dialog		
tag		local tag of the dialog ID		
To				RFC 3261 [15]
addr-spec		SIP URI of the SS which must be the same URI as used for the UE in the earlier requests within the dialog		
tag		remote tag of the dialog ID		
Call-ID				RFC 3261 [15]
callid		same value as in the first INVITE during the call setup		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the UE within its previous request in the same dialog but increased by one		
method		*REFER*		
Require	A1			RFC 3261 [15] RFC 3312 [31] RFC 3329 [21]
option-tag		*sec-agree*		
Proxy-Require	A1			RFC 3261 [15]
option-tag		*sec-agree*		RFC 3329 [21]
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as Security-Server header sent by SS		
Security-Verify	A2	not present		RFC 3329 [21]
Contact				RFC 3261 [15] RFC 5627 [61]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of UE		
	A2	SIP URI with IP address or FQDN and unprotected server port of UE		
	A3	Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response		
Refer-To				RFC 3515 [72]
addr-spec		SIP or Tel URI of the transfer target (Note 1)		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1,A2(o)			RFC 7315 [132] RFC 7913 [154]
access-net-spec	A4	access network information and, if applicable, the cell ID		
	A5	access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	Rel-15	
Content-Length		header shall be present if UE uses TCP to send this request and if there is a message-body		RFC 3261 [15]
value		length of message-body		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A4	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A5	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

NOTE 1: The SIP URI may contain a "Replaces" header referring to the dialog ID which has been established before.

A.2.11 MT NOTIFY for refer package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *NOTIFY* same URI value which the UE sent in its Contact header within the REFER request *SIP/2.0*		RFC 3261 [15]
Via via-parm1: sent-protocol sent-by sent-by via-branch via-parm2:	 A1 A2	order of the parameters in this header must be like in this table *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP IP address and protected server port of SS IP address and unprotected server port of SS (optional) value starting with '*z9hG4bK'* (NOTE 1) In addition to the via-parm entry for the SS, the following via-parm entries are included: *SIP/2.0/UDP scscf1.3gpp.org;branch=z9hG4bK...,* *SIP/2.0/UDP scscf2.3gpp.org;branch=z9hG4bK...,* *SIP/2.0/UDP pcscf2.3gpp.org;branch=z9hG4bK...,* *SIP/2.0/UDP uas.3gpp.org:6543;branch=z9hG4bK...* (NOTE 1)		RFC 3261 [15]
From addr-spec tag		 SIP URI of the SS which must be the same URI as used for the SS in the earlier requests within the dialog local tag of the dialog ID		RFC 3261 [15]
To addr-spec tag		 SIP URI of the UE which must be the same as used for the UE in the earlier requests within the dialog. remote tag of the dialog ID		RFC 3261 [15]
Call-ID callid		 same value as in the INVITE (and REFER) message		RFC 3261 [15]
CSeq value method	A1,A2	 value of CSeq sent by the SS within its previous request in the same dialog but increased by one *NOTIFY*		RFC 3261 [15]
Contact addr-spec addr-spec	 A1 A2	 SIP URI with IP address or FQDN and protected server port of the SS (transferee) SIP URI with IP address or FQDN and unprotected server port of the SS (transferee)		RFC 3261 [15]
Event event-type	A1,A2	 *refer*		RFC 6665 [140] RFC 3515 [72]
Max-Forwards value		 *69*		RFC 3261 [15]
Subscription-State substate-value expires		 *active* *300*		RFC 6665 [140]
Content-Type media-type		 *message/sipfrag*		RFC 3261 [15] RFC 3680 [22]
Content-Length value		 length of message-body		RFC 3261 [15] RFC 3680 [22]

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.2.12 MT REFER

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *REFER* same URI value as that which the UE has earlier sent in its Contact header within the dialog created by the INVITE sent by the UE when initiating the call to be transferred *SIP/2.0*		RFC 3261 [15]
Via via-parm1: sent-protocol sent-by sent-by via-branch via-parm2:	 A1 A2	order of the parameters in this header must be like in this table *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP IP address and protected server port of SS IP address and unprotected server port of SS (optional) value starting with '*z9hG4bK'* In addition to the via-parm entry for the SS, the following via-parm entries are included: *SIP/2.0/UDP scscf1.3gpp.org;branch=z9hG4bK...,* *SIP/2.0/UDP scscf2.3gpp.org;branch=z9hG4bK...,* *SIP/2.0/UDP pcscf2.3gpp.org;branch=z9hG4bK...,* *SIP/2.0/UDP uas.3gpp.org:6543;branch=z9hG4bK...* (NOTE 1)		RFC 3261 [15]
From addr-spec tag		 SIP URI of the SS which must be the same URI as used for the SS in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred local tag of the dialog ID		RFC 3261 [15]
To addr-spec tag		 SIP URI of the UE which must be the same URI as used for UE in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred remote tag of the dialog ID		RFC 3261 [15]
Call-ID callid		 same value as in the first INVITE sent by the UE during setup of the call to be transferred		RFC 3261 [15]
CSeq value method		 value of CSeq sent by the SS within its previous request in the dialog created by the INVITE sent by the UE when initiating the call to be transferred, but increased by one *REFER*		RFC 3261 [15]
Contact addr-spec	 A1 A2	 SIP URI with IP address or FQDN and protected server port of the SS (transferor) SIP URI with IP address or FQDN and unprotected server port of the SS (transferor)		RFC 3261 [15]
Refer-To addr-spec		 SIP or Tel URI of the transfer target		RFC 3515 [72]
Max-Forwards value		 non-zero value		RFC 3261 [15]
Content-Length value		 length of message-body		RFC 3261 [15]

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5])
A2	GIBA (A.6a/1 TS 34.229-2 [5])

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.2.13 MO NOTIFY for refer package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI		same URI value which the SS sent in its Contact header within the REFER request		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address or FQDN and protected server port of the UE		
	A2	IP address or FQDN and unprotected server port of UE		
via-branch		value starting with '*z9hG4bK*'		
Route		order of the parameters in this header must be like in the respective rows		RFC 3261 [15]
route-param	A1	<*sip:*SS P-CSCF address: protected server port of SS *;lr>, <sip:scscf.3gpp.org;lr>*		
	A2	<*sip:*SS P-CSCF address: unprotected server port of SS (optional)*;lr>, <sip:scscf.3gpp.org;lr*		
From				RFC 3261 [15]
addr-spec		Local SIP URI of the UE which must be the same URI as used for the UE in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred		
tag		local tag of the dialog ID		
To				RFC 3261 [15]
addr-spec		Remote SIP URI of the SS which must be the same as used for the SS in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred.		
tag		remote tag of the dialog ID		
Call-ID				RFC 3261 [15]
callid		same value as in the INVITE (and REFER) message		
CSeq	A1,A2			RFC 3261 [15]
value		value of CSeq sent by the SS within its previous request in the dialog created by the INVITE sent by the UE when initiating the call to be transferred, but increased by one		
method		*NOTIFY*		
Contact				RFC 3261 [15] RFC 5627 [61]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of the UE or GRUU as returned by the SS in registration		
	A2	SIP URI with IP address or FQDN and unprotected server port of UE or GRUU as returned by the SS in registration		
	A3	Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response		
Event	A1,A2			RFC 6665 [140] RFC 3515 [72]
event-type		*refer*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Subscription-State				RFC 6665 [140]
substate-value		*active*		
expires		non-zero value		
Content-Type				RFC 3261 [15] RFC 3680 [22]
media-type		*message/sipfrag*		
Content-Length		header shall be present if UE uses TCP to send this request and if there is a message-body		RFC 3261 [15] RFC 3680 [22]
value		length of message-body		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5])
A2	GIBA (A.6a/1 TS 34.229-2 [5])

A3	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])

A.2.14 181 Call is being forwarded

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*181*		
Reason-Phrase		*Call is being forwarded*		
Via				RFC 3261 [15]
via-parm		same value as received in INVITE message		
From				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		local tag of the dialog ID		
To				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		remote tag of the dialog ID		
History-Info				RFC 7044 [83]
hi-targeted-to-uri		*<sip:user@company.com>*		
hi-index		*1*		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		same value as received in INVITE message		
Content-Length				RFC 3261 [15]
value		0		

A.2.15 CANCEL

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*CANCEL*		
Request-URI		same value as in the INVITE being cancelled		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
via-parm		same value as in the INVITE being cancelled		
From				RFC 3261 [15]
addr-spec		same value as in the INVITE being cancelled		
tag		same value as in the INVITE being cancelled		
To				RFC 3261 [15]
addr-spec		same value as in the INVITE being cancelled		
Call-ID				RFC 3261 [15]
callid		same value as in the INVITE being cancelled		
CSeq				RFC 3261 [15]
value		same value as received in INVITE message		
method		*CANCEL*		
Content-Length				RFC 3261 [15]
value		*0*		

A.2.16 487 Request Terminated

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *487* *Request Terminated*		RFC 3261 [15]
Via via-parm		 same value as received in INVITE message		RFC 3261 [15]
From addr-spec tag		 same value as received in INVITE message same value as received in INVITE message		RFC 3261 [15]
To addr-spec tag		 same value as received in INVITE message same value as in 200 OK for the corresponding CANCEL request		RFC 3261 [15]
Call-ID callid		 same value as received in INVITE message		RFC 3261 [15]
CSeq value		 same value as received in INVITE message		RFC 3261 [15]
Content-Length value		optional when sent by UE 0		RFC 3261 [15]

A.2.17 404 Not Found

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *404* *Not Found*		RFC 3261 [15]
Via via-parm		 same value as received in INVITE message		RFC 3261 [15]
From addr-spec tag		 same value as received in INVITE message same value as received in INVITE message		RFC 3261 [15]
To addr-spec tag		 same value as received in INVITE message same value as in an earlier responses sent to the UE for this dialog		RFC 3261 [15]
Call-ID callid		 same value as received in INVITE message		RFC 3261 [15]
CSeq value		 same value as received in INVITE message		RFC 3261 [15]
Content-Length value		 0		RFC 3261 [15]

A.2.18 481 Call/Transaction Does Not Exist

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*481*		
Reason-Phrase		Call/Transaction Does Not Exist		
Via				RFC 3261 [15]
via-parm		same value as received in request		
From				RFC 3261 [15]
addr-spec		same value as received in request		
tag		same value as received in request		
To				RFC 3261 [15]
addr-spec		same value as received in request		
tag		any arbitrary tag value added		
Call-ID				RFC 3261 [15]
callid		same value as received in request		
CSeq				RFC 3261 [15]
value		same value as received in request		
Content-Length				RFC 3261 [15]
value		0		

A.2.19 MO INFO for eCall over IMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*INFO*		RFC 6086 [139]
Request-URI	A1	*urn:service:sos.ecall.manual*	Rel-14	TS 24.229 [10] RFC 8147 [149]
	A2	*urn:service:sos.ecall.automatic*	Rel-14	TS 24.229 [10] RFC 8147 [149]
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15] RFC 3581 [96]
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		IP address or FQDN and protected server port of the UE		
via-branch		value starting with '*z9hG4bK'*		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE		TS 24.229 [10]
tag		local tag of the dialog ID		
To				RFC 3261 [15]
addr-spec	A1	*urn:service:sos.ecall.manual*	Rel-14	TS 24.229 [10] RFC 8147 [149]
	A2	*urn:service:sos.ecall.automatic*	Rel-14	TS 24.229 [10] RFC 8147 [149]
tag		remote tag of the dialog ID		
Call-ID				RFC 3261 [15]
callid		same as value received in INVITE message		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the UE within its previous request in the same dialog but increased by one		
method		*INFO*		
Call-Info				
cid URL		any URL	Rel-14	RFC 8147 [149]
purpose		*EmergencyCallData.eCall.MSD*	Rel-14	RFC 8147 [149]
Info-Package		*EmergencyCallData.eCall.MSD*	Rel-14	RFC 8147 [149]
Content-Type				RFC 3261 [15]
media-type		*multipart/mixed;boundary*=any value		TS 24.229 [10]
Content-Length				RFC 3261 [15]
value		length of message-body		
Content-Disposition				RFC 3261 [15]
disp-type		*Info-Package*	Rel-14	RFC 8147 [149]
Message-body				
	A3	--boundary value (as provided in Content-Type) *Content-Type: application/EmergencyCallData.eCall.MSD* *Content-ID: same cid as in Call-Info header* *Content-Disposition: by-reference* MSD in ASN.1 PER encoding --boundary value (as provided in Content-Type)	Rel-14	RFC 8147 [149]
	A4	--boundary value (as provided in Content-Type) *Content-Type: application/EmergencyCallData.eCall.Control+xml* *Content-ID: same cid as in Call-Info header* *Content-Disposition: by-reference* *<?xml version="1.0" encoding="UTF-8"?>* *<EmergencyCallData.Control xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control"*> <*ack ref*=cid of the body part of corresponding INFO request from SS> *<actionResult action="send-data" success="false" reason*=any value/> *</ack>* *</EmergencyCallData.Control*> --boundary value (as provided in Content-Type)	Rel-14	RFC 8147 [149]

Condition	Explanation
A1	eCall over IMS was started manually
A2	eCall over IMS was started automatically

A3	UE able to provide an updated MSD
A4	UE not able to provide an updated MSD

A.2.20 MT INFO for eCall over IMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *INFO* same URI as UE sent in Contact header of INVITE *SIP/2.0*		RFC 3261 [15] RFC 6086 [139] RFC 8147 [149]
Via via-parm1: sent-protocol sent-by via-branch via-parm2: sent-protocol sent-by via-branch		order of the parameters in this header must be like in this table *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP IP address and protected server port of SS value starting with '*z9hG4bK'* *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP *psap.3gpp.org* value starting with '*z9hG4bK'*		RFC 3261 [15] RFC 3581 [96]
From addr-spec tag		 SIP URI of PSAP remote tag of the dialog ID		RFC 3261 [15] TS 24.229 [10] RFC 8147 [149]
To addr-spec tag		 SIP URI of UE local tag of the dialog ID		RFC 3261 [15] TS 24.229 [10] RFC 8147 [149]
Call-ID callid		 same as value received in INVITE message		RFC 3261 [15]
CSeq value method		 value of CSeq sent by the SS within its previous request in the same dialog but increased by one. If this is first request sent by SS, any value is used (e.g. 4711). *INFO*		RFC 3261 [15]
Call-Info cid URL purpose		 *test-info@3gpp.org* *EmergencyCallData.Control*	 Rel-14 Rel-14	 RFC 8147 [149] RFC 8147 [149]
Info-Package		*EmergencyCallData.eCall.MSD*	Rel-14	RFC 8147 [149]
Content-Type media-type		 *multipart/mixed;boundary=boundaryXXX*	 Rel-14	RFC 3261 [15] TS 24.229 [10]
Content-Length value		 length of message-body		
Content-Disposition disp-type		 *Info-Package*	 Rel-14	 RFC 8147 [149]
Message-body		*--boundaryXXX* *Content-Type: application/EmergencyCallData.Control+xml* *Content-ID: test-info@3gpp.org* *Content-Disposition: by-reference* <?xml version="1.0" encoding="UTF-8"?> <EmergencyCallData.Control xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control"> <request action="send-data" datatype="eCall.MSD"/> </EmergencyCallData.Control> *--boundaryXXX*	Rel-14	RFC 8147 [149]

A.2.21 486 Busy Here

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *486* *Busy Here*		RFC 3261 [15]
Via via-parm		 same value as received in request		RFC 3261 [15]
From addr-spec tag		 same value as received in request same value as received in request		RFC 3261 [15]
To addr-spec tag		 same value as received in request any arbitrary tag value added		RFC 3261 [15]
Call-ID callid		 same value as received in request		RFC 3261 [15]
CSeq value		 same value as received in request		RFC 3261 [15]
Recv-Info Info-package-type	A1	 *emergencyCallData.eCall.MSD*		 RFC 8147 [149]
Call-Info cid URL purpose	A1	 *test-486@3gpp.org* *EmergencyCallData.eCall.Control*		 RFC 8147 [149] RFC 8147 [149]
Accept media-range	A1	 *application/sdp,* *application/pidf+xml,* *application/EmergencyCallData.Control+xml,* *application/emergencyCallData.eCall.MSD*		 RFC 8147 [149]
Content-Type media-type	A1	 *multipart/mixed;boundary=boundary1*		 RFC 8147 [149]
Content-Length value		 length of message body		RFC 3261 [15]
Message-body	A1	*--boundary1* *Content-Type: application/EmergencyCallData.eCall.Control+xml* *Content-ID:* test-486@3gpp.org *Content-Disposition: by-reference* *<?xml version="1.0" encoding="UTF-8"?>* *<EmergencyCallData.Control xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control">* *<ack received="true" ref="*cid URL of MIME body part containing the MSD sent by the UE in INVITE*"/>* *</EmergencyCallData.Control>* *--boundary1*		RFC 8147 [149]

Condition	Explanation
A1	Response sent by SS for INVITE for eCall over IMS

A.2.22 600 Busy Everywhere

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *600* *Busy Everywhere*		RFC 3261 [15]
Via via-parm		 same value as received in request		RFC 3261 [15]
From addr-spec tag		 same value as received in request same value as received in request		RFC 3261 [15]
To addr-spec tag		 same value as received in request any arbitrary tag value added		RFC 3261 [15]
Call-ID callid		 same value as received in request		RFC 3261 [15]
CSeq value		 same value as received in request		RFC 3261 [15]
Recv-Info Info-package-type	A1	 *emergencyCallData.eCall.MSD*	 Rel-14	 RFC 8147 [149]
Call-Info cid URL purpose	A1	 *test-600@3gpp.org* *EmergencyCallData.eCall.Control*	 Rel-14	 RFC 8147 [149]
Accept media-range	A1	 *application/sdp,* *application/pidf+xml,* *application/EmergencyCallData.Control+xml,* *application/emergencyCallData.eCall.MSD*	 Rel-14	 RFC 8147 [149]
Content-Type media-type	A1	 *multipart/mixed;boundary=boundary1*	 Rel-14	 RFC 8147 [149]
Content-Length value		 length of message body		RFC 3261 [15]
Message-body	A1	*--boundary1* *Content-Type:* *application/EmergencyCallData.eCall.Control+xml* *Content-ID:* test-600@3gpp.org *Content-Disposition: by-reference* *<?xml version="1.0" encoding="UTF-8"?>* *<EmergencyCallData.Control* *xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control">* *<ack received="true" ref="*cid URL of MIME body part containing the MSD sent by the UE in INVITE*"/>* *</EmergencyCallData.Control>* *--boundary1*	Rel-14	RFC 8147 [149]

Condition	Explanation
A1	Response sent by SS for INVITE for eCall over IMS

A.2.23 603 Decline

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *603* *Decline*		RFC 3261 [15]
Via via-parm		 same value as received in request		RFC 3261 [15]
From addr-spec tag		 same value as received in request same value as received in request		RFC 3261 [15]
To addr-spec tag		 same value as received in request any arbitrary tag value added		RFC 3261 [15]
Call-ID callid		 same value as received in request		RFC 3261 [15]
CSeq value		 same value as received in request		RFC 3261 [15]
Recv-Info Info-package-type	 A1	 *emergencyCallData.eCall.MSD*	 Rel-14	RFC 6086 [139] RFC 8147 [149]
Call-Info cid URL purpose	 A1 A1	 *test-603@3gpp.org* *EmergencyCallData.eCall.Control*	 Rel-14 Rel-14	 RFC 8147 [149]
Accept media-range		 *application/sdp,* *application/pidf+xml,* *application/EmergencyCallData.Control+xml,* *application/emergencyCallData.eCall.MSD*	 Rel-14	 RFC 8147 [149]
Content-Type media-type	 A1	 *multipart/mixed;boundary=boundary1*		 RFC 8147 [149]
Content-Length value		 length of message body		RFC 3261 [15]
Message-body	A1	*--boundary1* *Content-Type:* *application/EmergencyCallData.eCall.Control+xml* *Content-ID*: *test-603@3gpp.org* *Content-Disposition: by-reference* *<?xml version="1.0" encoding="UTF-8"?>* *<EmergencyCallData.Control* *xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control"*> *<ack received="true" ref=*"cid URL of MIME body part containing the MSD sent by the UE in INVITE*"/>* *</EmergencyCallData.Control*> *--boundary1*	Rel-14	RFC 8147 [149]

Condition	Explanation
A1	Response sent by SS for INVITE for eCall over IMS

A.2.24 422 Session Interval Too Small

Header/param	Cond	Value/remark	Rel	Reference
Status-Line			Rel-8	RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*422*		RFC 4028 [146]
Reason-Phrase		*Session Interval Too Small*		RFC 4028 [146]
Via			Rel-8	RFC 3261 [15]
via-parm		same value as received in request		
From			Rel-8	RFC 3261 [15]
addr-spec		same value as received in request		
tag		same value as received in request		
To			Rel-8	RFC 3261 [15]
addr-spec		same value as received in request		
tag		any arbitrary tag value added		
Call-ID			Rel-8	RFC 3261 [15]
callid		same value as received in request		
CSeq			Rel-8	RFC 3261 [15]
value		same value as received in request		
Min-SE			Rel-8	RFC 4028 [146]
delta-seconds		value shall be greater than or equal to 90		
Content-Length			Rel-8	RFC 3261 [15]
value		0		

A.3 Generic Common Messages

A.3.1 200 OK for other requests than REGISTER or SUBSCRIBE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *200* *OK*		RFC 3261 [15]
Via via-parm		not present same value as received in request		RFC 3261 [15]
Record-Route rec-route	 A1 A3 A2,A4, A5 A6 A7	order of the parameters in this header must be like in the respective rows *<sip:pcscf.other.com;lr>, <sip:scscf.other.com;lr>, <sip:orig@scscf.3gpp.org;lr>, <sip:*SS P-CSCF address: protected server port of SS*;lr>* *<sip:pcscf.other.com;lr>, <sip:scscf.other.com;lr>, <sip:orig@scscf.3gpp.org;lr>, <sip:*SS P-CSCF address: unprotected server port of SS (optional)*;lr>* same value as received in the request (if present in the request) Note: for requests other than INVITE it is not regulated if and what the UE writes into this header in a response. *<sip:orig@ecscf.other.com;lr>, <sip:*SS P-CSCF address*:*protected server port of SS*;lr>* *<sip:orig@ecscf.other.com;lr>, <sip:*SS P-CSCF address*:*unprotected server port of SS*;lr>*		RFC 3261 [15]
From addr-spec tag		 same value as received in request same value as received in request		RFC 3261 [15]
To addr-spec tag		 same value as received in request same value as received in request or any value added if missing from request		RFC 3261 [15]
P-Asserted-Identity addr-spec uri-parameter		 A tel URI that can be recognized as valid emergency numbers if dialled by the user are specified in 3GPP TS 22.101 [39]. The emergency numbers 112 and 911 are stored on the ME, in accordance with 3GPP TS 22.101 [39] *lr*		RFC 3325 [89]
Contact addr-spec feature-param	A1,A2 A3,A4 A1,A3 A2 AND NOT A9 A4 AND NOT A9 A2 AND A9 A4 AND A9 A10 A18 AND (A19 OR A20) A11 AND A14 AND (A15 OR A16)	 px_IMS_CalleeContactUri SIP URI with IP address or FQDN and protected server port of UE SIP URI with IP address or FQDN and unprotected server port of UE Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response *audio* *video* *audio*		RFC 3261 [15] RFC 5627 [61 IR.94 [134]
Call-ID callid		 same value as received in request		RFC 3261 [15]
Call-Info cid URL purpose		 *psap@3gpp.org* *EmergencyCallData.Control*	 Rel-14	RFC 8147 [149]

CSeq value		 same value as received in request		RFC 3261 [15]
P-Access-Network-Info access-net-spec	A8 A21	 access network information and, if applicable, the cell ID		RFC 7315 [132] RFC 7913 [154]
	A22	access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID		
Accept media-range		 *application/sdp, application/pidf+xml, application/EmergencyCallData.Control+xml, application/emergencyCallData.eCall.MSD*	 Rel-14	RFC 8147 [149]
Recv-Info Info-package-type	 A12	 *emergencyCallData.eCall.MSD*	 Rel-14	RFC 8147 [149]
Content-Type media-type	 A12	 *multipart/mixed; boundary=boundary1*	 Rel-14	RFC 8147 [149]
Content-Length value	A10 NOT A12 A12	 0 length of message body		RFC 3261 [15]
Message-body	 A13 A14	 *--boundary1* *Content-Type: application/EmergencyCallData.eCall.Control+xml* *Content-ID:* same cid as in Call-Info header *Content-Disposition: by-reference* *<?xml version="1.0" encoding="UTF-8"?>* *<EmergencyCallData.control xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control">* *<ack received="true" ref=" cid URL of MIME body part containing the MSD sent by the UE in INVITE"/>* *</EmergencyCallData.control>* *--boundary1* *--boundary1* *Content-Type: application/EmergencyCallData.eCall.Control+xml* *Content-Disposition: by-reference* *<?xml version="1.0" encoding="UTF-8"?>* *<emergencyCallData.Control xmlns="urn:ietf:params:xml:ns:EmergencyCallData:control">* *<ack received="false" ref=" cid URL of MIME body part containing the MSD sent by the UE in INVITE "/>* *</EmergencyCallData.control>* *--boundary1*		 RFC 8147 [149] RFC 8147 [149]

Condition	Explanation
A1	Response sent by SS for INVITE/UPDATE (IMS security, A.6a/2 TS 34.229-2 [5]))
A2	Response sent by UE for INVITE/UPDATE (IMS security, A.6a/2 TS 34.229-2 [5]))
A3	Response sent by SS for INVITE/UPDATE (GIBA, A.6a/1 TS 34.229-2 [5]))
A4	Response sent by UE for INVITE/UPDATE (GIBA, A.6a/1 TS 34.229-2 [5]))
A5	Any response sent by the UE within a dialog
A6	Response sent by SS for INVITE for emergency call or non-UE detectable emergency call
A7	Response sent by SS for INVITE for emergency call without emergency registration
A8	Any response sent by the UE within a dialog, except for CANCEL requests
A9	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A10	Response sent by SS
A11	Response sent by UE
A12	Response sent by SS for INVITE for eCall over IMS session with either ACK or NACK
A13	Response sent by SS for INVITE for eCall over IMS session with ACK element = TRUE
A14	Response sent by SS for INVITE for eCall over IMS session with ACK element = FALSE
A15	UE supports audio media feature tag (A.12/56 3GPP TS 34.229-2 [5])
A16	UE uses E-UTRAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.301 [150], clauses 8.2.1 and 9.9.3.12A
A17	UE uses UTRAN/GERAN access and has received IMS voice over PS Session Supported Indication in the NAS ATTACH ACCEPT message as described in TS 24.008 [12], clauses 9.4.2 and 10.5.5.23
A18	UE supports video feature tag (A.12/32 3GPP TS 34.229-2 [5])
A19	Response sent by SS for INVITE
A20	Response sent by UE for INVITE
A21	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A22	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

A.3.2 403 FORBIDDEN

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *403* *Forbidden*		RFC 3261 [15]
Via via-parm		 same value as received in the previous REGISTER message		RFC 3261 [15]
To addr-spec tag		 same value as received in the previous REGISTER message common to-tag (register)		RFC 3261 [15]
From addr-spec		 same value as received in the previous REGISTER message		RFC 3261 [15]
Call-ID value		 same value as received in the previous REGISTER message		RFC 3261 [15]
CSeq value		 same value as received in the previous REGISTER message		RFC 3261 [15]
Content-Type media-type	A1	 *application/3gpp-ims+xml*		RFC 3261 [15]
Content-Length value		 *0*		RFC 3261 [15]
Message-body	A1	*<?xml version="1.0" encoding="UTF-8"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>emergency</type>* *<action>anonymous-emergencycall</action>* *<reason></reason>* *</alternative-service>* *</ims-3gpp>* (see NOTE 1)		RFC 3261 [15]

Condition	Explanation
A1	IMS emergency call for an anonymous emergency call

NOTE 1: This XML body is defined in Rel-14 TS 24.229 [10] and may be ignored by pre-Rel-14 UE.

A.3.3 202 Accepted

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *202* *Accepted*		RFC 3261 [15]
Via via-parm		 same value as received in request		RFC 3261 [15]
From addr-spec tag		 same value as received in request same value as received in request		RFC 3261 [15]
To addr-spec tag		 same value as received in request same value as received in request or common to-tag (message) added if missing from request		RFC 3261 [15]
Call-ID callid		 same value as received in request		RFC 3261 [15]
CSeq value		 same value as received in request		RFC 3261 [15]
Content-Length value		optional when sent by the UE *0*		RFC 3261 [15]

A.4 Other Default Messages

A.4.1 380 Alternative Service

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *380* *Alternative Service*		RFC 3261 [15]
Via via-parm		 same value as received in request		RFC 3261 [15]
From addr-spec tag		 same value as received in request same value as received in request		RFC 3261 [15]
To addr-spec tag		 same value as received in request same value as received in request or common to-tag (invite) added if missing from request		RFC 3261 [15]
P-Asserted-Identity addr-spec uri-parameter		 SS P-CSCF address *lr*		RFC 3325 [89]
Call-ID callid		 same value as received in request		RFC 3261 [15]
CSeq value		 same value as received in request		RFC 3261 [15]
Content-Type media-type		 *application/3gpp-ims+xml*		RFC 3261 [15]
Content-Length value		 length of message-body		RFC 3261 [15]
Message-body		*<?xml version="1.0" encoding="UTF-8"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>emergency</type>* *<reason></reason>* *</alternative-service>* *</ims-3gpp>*		

A.4.2 503 Service Unavailable

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*503*		
Reason-Phrase		*Service Unavailable*		
Via				RFC 3261 [15]
via-parm		same value as received in request		
From				RFC 3261 [15]
addr-spec		same value as received in request		
tag		same value as received in request		
To				RFC 3261 [15]
addr-spec		same value as received in request		
tag		any arbitrary tag value added		
Call-ID				RFC 3261 [15]
callid		same value as received in request		
CSeq				RFC 3261 [15]
value		same value as received in request		
Retry-After				RFC 3261 [15] TS 24.229 [10], 5.1.2.2
period		*60* (referred to as T in the test procedure and test requirement)		
duration		not present		
comment		not present		
Content-Length				RFC 3261 [15]
value		*0*		

A.4.3 PUBLISH

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *PUBLISH* any IMPU within the set of IMPUs on ISIM *SIP/2.0*		RFC 3261 [15] RFC 3903 [60]
Route route-param	 A1 A2	order of the parameters in this header must be like in the respective rows <*sip:*SS P-CSCF address:protected server port of P-CSCF*;lr*>, <*sip:scscf.3gpp.org;lr*> <*sip:*SS P-CSCF address: unprotected server port of P-CSCF (optional)*;lr*>, <*sip:scscf.3gpp.org;lr*>		RFC 3261 [15]
Via sent-protocol sent-by sent-by via-branch	 A1 A2	 *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP IP address or FQDN and protected server port of the UE IP address or FQDN, port (optional) and not checked value starting with '*z9hG4bK*'		RFC 3261 [15]
From addr-spec tag		 any IMPU within the set of IMPUs on ISIM must be present, value not checked but stored for later reference		RFC 3261 [15]
To addr-spec tag		 any IMPU within the set of IMPUs on ISIM not present		RFC 3261 [15]
Expires delta-seconds		optional same as registration timer		RFC 3261 [15]
Security-Verify sec-mechanism	A1	 same value as Security-Server header sent by SS		
Require option-tag	A1	optional value not checked		RFC 3261 [15] RFC 3329 [21]
Proxy-Require option-tag	A1	optional value not checked		RFC 3261 [15] RFC 3329 [21]
CSeq value method		 must be present, value not checked *PUBLISH*		RFC 3261 [15]
Call-ID callid		 value not checked, but stored for later reference		RFC 3261 [15]
Max-Forwards value		 non-zero value		RFC 3261 [15]
P-Access-Network-Info access-net-spec	A1 A4 A5	 access network information and, if applicable, the cell ID access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID		RFC 7315 [132] RFC 7913 [154]
Event event-type		 value not checked		RFC 6665 [140] RFC 3680 [22] RFC 3903 [60]
SIP-If-Match entity-tag		optional		RFC 3903 [60]
Content-Length value		header shall be present if UE uses TCP to send this request and if there is a message-body length of request body, if such is present		RFC 3261 [15]
Message-body		optional		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))
A3	Void
A4	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])

A5	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

A.4.4 200 OK for PUBLISH

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*200*		
Reason-Phrase		*OK*		
Via				RFC 3261 [15]
via-parm		same value as received in PUBLISH message		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		common to-tag (subscribe dialog)		
From				RFC 3261 [15]
addr-spec		same value as received in PUBLISH message		
tag		same value as received in PUBLISH message		
Call-ID				RFC 3261 [15]
callid		same value as received in PUBLISH message		
CSeq				RFC 3261 [15]
value		same value as received in PUBLISH message		
Contact				RFC 3261 [15]
addr-spec		*<sip:scscf.3gpp.org>*		
Expires				RFC 3261 [15] RFC 3903 [60]
delta-seconds		*600000*		
SIP-ETag				RFC 3903 [60]
entity-tag		unique, generated tag for every request		
Content-Length				RFC 3261 [15]
value		*0*		

A.4.5 302 Moved Temporarily

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*302*		
Reason-Phrase		*Moved Temporarily*		
Via				RFC 3261 [15]
via-parm		same value as received in request		
From				RFC 3261 [15]
addr-spec		same value as received in request		
tag		same value as received in request		
To				RFC 3261 [15]
addr-spec		same value as received in request		
tag		any arbitrary tag value added		
Call-ID				RFC 3261 [15]
callid		same value as received in request		
Contact				RFC 3261 [15]
addr-spec		*sip:user@company.com*		
CSeq				RFC 3261 [15]
value		same value as received in request		
Content-Length				RFC 3261 [15]
value		*0*		

A.4.6 504 Server Time-out

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *504* *Server Time-out*		RFC 3261 [15]
Via via-parm		 same value as received in request		RFC 3261 [15]
From addr-spec tag		 same value as received in request same value as received in request		RFC 3261 [15]
To addr-spec tag		 same value as received in request any arbitrary tag value added		RFC 3261 [15]
P-Asserted-Identity addr-spec uri-parameter		 *scscf.3gpp.org* *lr*		RFC 3325 [89]
Call-ID callid		 same value as received in request		RFC 3261 [15]
CSeq value		 same value as received in request		RFC 3261 [15]
Content-Length value		 length of message-body		RFC 3261 [15]
Content-Type media-type		 *application/3gpp-ims+xml*		RFC 3261 [15]
Message-body		*<?xml version="1.0" encoding="UTF-8"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>restoration</type>* *<reason/>* *<action>initial-registration</action>* *</alternative-service>* *</ims-3gpp>*		

A.4.7 500 Server Internal Error

Header/param	Cond	Value/remark	Rel	Reference
Status-Line SIP-Version Status-Code Reason-Phrase		 *SIP/2.0* *500* *Server Internal Error*		RFC 3261 [15]
Via via-parm		 same value as received request		RFC 3261 [15]
From addr-spec tag		 same value as received in request same value as received in request		RFC 3261 [15]
To addr-spec tag		 same value as received in request any arbitrary tag value added		RFC 3261 [15]
Call-ID value		 same value as received in request		RFC 3261 [15]
CSeq value		 same value as received in request		RFC 3261 [15]
Content-Length value		 *0*		RFC 3261 [15]

A.4.8 305 Use Proxy

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*305*		
Reason-Phrase		*Use Proxy*		
Via				RFC 3261 [15]
via-parm		same value as received request		
From				RFC 3261 [15]
addr-spec		same value as received in request		
tag		same value as received in request		
To				RFC 3261 [15]
addr-spec		same value as received in request		
tag		any arbitrary tag value added		
Call-ID				RFC 3261 [15]
value		same value as received in request		
CSeq				RFC 3261 [15]
value		same value as received in request		
Content-Length				RFC 3261 [15]
value		*0*		

A.5 Default messages for Conferencing

A.5.1 SUBSCRIBE for conference event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*SUBSCRIBE*		
Request-URI		*sip:final@conf-factory.* appended with px_IMS_HomeDomainName		
SIP-Version		*SIP/2.0*		
Route		order of the parameters in this header must be like in the respective rows		RFC 3261 [15]
route-param	A1	<*sip:*SS P-CSCF address:protected server port of P-CSCF*;lr>, <sip:scscf.3gpp.org;lr>*		
	A2	<*sip:*SS P-CSCF address: unprotected server port of P-CSCF (optional)*;lr>, <sip:scscf.3gpp.org;lr>*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address or FQDN and protected server port of the UE		
sent-by	A2	IP address or FQDN and unprotected server port of the UE		
via-branch		value starting with '*z9hG4bK'*		
From				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		must be present, value not checked but stored for later reference		
To				RFC 3261 [15]
addr-spec		*sip:final@conf-factory.* appended with px_IMS_HomeDomainName		
tag		not present		
Contact				RFC 3261 [15] RFC 5627 [61]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of UE		
	A2	SIP URI with IP address or FQDN and unprotected server port of UE		
	A4	Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response		
Expires				RFC 3261 [15]
delta-seconds		must be present but value not checked		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as Security-Server header sent by SS		
Require	A1			RFC 3261 [15]
option-tag		*sec-agree*		RFC 3329 [21]
Proxy-Require	A1			RFC 3261 [15]
option-tag		*sec-agree*		RFC 3329 [21]
CSeq				RFC 3261 [15]
value		must be present, value not checked		
method		*SUBSCRIBE*		
Call-ID				RFC 3261 [15]
callid		value not checked, but stored for later reference		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1			RFC 7315 [132] RFC 7913 [154]
access-net-spec	A6	access network information and, if applicable, the cell ID		
	A7	access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	Rel-15	
Accept				RFC 3261 [15]
media-range		*application/conference-info+xml*		RFC 3680 [22]
Event				RFC 6665 [140] RFC 3680 [22]
event-type		*conference*		
Content-Length		header shall be present if UE uses TCP to send this request and if there is a message-body		RFC 3261 [15]
value		length of request body, if such is present		

Condition	Explanation

A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))
A3	Void
A4	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A5	Void.
A6	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A7	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

A.5.2 200 OK for SUBSCRIBE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*200*		
Reason-Phrase		*OK*		
Via				RFC 3261 [15]
via-parm		same value as received in SUBSCRIBE message		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		common to-tag (subscribe conference dialog)		
From				RFC 3261 [15]
addr-spec		same value as received in SUBSCRIBE message		
tag		same value as received in SUBSCRIBE message		
Call-ID				RFC 3261 [15]
callid		same value as received in SUBSCRIBE message		
CSeq				RFC 3261 [15]
value		same value as received in SUBSCRIBE message		
Contact				RFC 3261 [15]
addr-spec		*sip:final@conf-factory.* appended with px_IMS_HomeDomainName		
Expires				RFC 3261 [15]
delta-seconds		*7200*		
Record-Route				RFC 3261 [15]
addr-spec	A1	SS P-CSCF address: protected server port of SS		
	A2	SS P-CSCF address: unprotected server port of SS (optional)		
uri-parameter		*lr*		
Content-Length				RFC 3261 [15]
value		*0*		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))

A.5.3 NOTIFY for conference event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI		UE's contact address in SIP URI form, as provided in the Contact header within the SUBSCRIBE creating the dialog		
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15]
via-parm1:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address and protected server port of SS		
sent-by	A2	IP address and unprotected server port of SS (optional)		
via-branch		value starting with '*z9hG4bK'* (NOTE 1)		
via-parm2:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		*scscf.3gpp.org*		
via-branch		value starting with '*z9hG4bK'* (NOTE 1)		
From				RFC 3261 [15]
addr-spec		*sip:final@conf-factory.* appended with px_IMS_HomeDomainName		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same as value received in SUBSCRIBE message		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the SS within its previous request in the same dialog but increased by one		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec		*sip:final@conf-factory.* appended with px_IMS_HomeDomainName		
Event				RFC 6665 [140] RFC 4575 [86]
event-type		*conference*		
Max-Forwards				RFC 3261 [15]
value		*69*		
Subscription-State				RFC 6665 [140]
substate-value	A3	*active*		
expires	A3	*7200*		
substate-value	A4	*terminated*		RFC 4575 [86]
reason	A4	*noresource*		RFC 6665 [140]
Content-Type	A3			RFC 3261 [15]
media-type		*application/conference-info+xml*		RFC 4575 [86]
Content-Length				RFC 3261 [15]
value		length of message-body		

Message-body	A3	*<?xml version="1.0" encoding="UTF-8"?>* *<conference-info* *xmlns="urn:ietf:params:xml:ns:conference-info">* *entity=*sip:final@conf-factory. appended with px_IMS_HomeDomainName *state="full" version="0">* *<users>* *<user entity="*any IMPU within the set of IMPUs on ISIM*">* *<endpoint entity="* Contact URI of the UE*">* *<status>connected</status>* *<joining-method>dialed-in</joining-method>* *<media id="1">* *<type>audio</type>* *<label>34567</label>* *<src-id>*SSRC of UE's RTP packets*</src-id>* *<status>sendrecv</status>* *</media>* *</endpoint>* *</user>* *</user>* *</conference-info>*		RFC 4575 [86]

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))
A3	SS sends NOTIFY to indicate that UE is now subscribed to the conference event package
A4	SS sends NOTIFY to indicate that UE’s subscription to conference event is terminated now

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.6 Default messages for Message Waiting Indication

A.6.1 SUBSCRIBE for message-summary event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *SUBSCRIBE* any IMPU within the set of IMPUs on ISIM or px_IMS_MessageAccountIdentity. UE shall use px_IMS_MessageAccountIdentity when that is configured to the phone as public service identity of the message account. *SIP/2.0*		RFC 3261 [15]
Route route-param	 A1 A2	order of the parameters in this header must be like in the respective rows <*sip:*SS P-CSCF address:protected server port of P-CSCF*;lr>, <sip:scscf.3gpp.org;lr>* <*sip:*SS P-CSCF address: unprotected server port of P-CSCF (optional)*;lr>, <sip:scscf.3gpp.org;lr>*		RFC 3261 [15]
Via sent-protocol sent-by sent-by via-branch	 A1 A2	 *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP IP address or FQDN and protected server port of the UE IP address or FQDN and unprotected server port of the UE value starting with '*z9hG4bK'*		RFC 3261 [15]
From addr-spec tag		 any IMPU within the set of IMPUs on ISIM must be present, value not checked but stored for later reference		RFC 3261 [15]
To addr-spec tag		 any IMPU within the set of IMPUs on ISIM or px_IMS_MessageAccountIdentity. UE shall use px_IMS_MessageAccountIdentity when that is configured to the phone as public service identity of the message account. not present		RFC 3261 [15]
Contact addr-spec	 A1 A2 A4	 SIP URI with IP address or FQDN and protected server port of UE SIP URI with IP address or FQDN and unprotected server port of UE Public GRUU as obtained during registration as pub-gruu contact parameter of the 200 OK for REGISTER response		RFC 3261 [15] RFC 5627 [61]
Expires delta-seconds		 must be present but value not checked		RFC 3261 [15]
Security-Verify sec-mechanism	A1	 same value as Security-Server header sent by SS		RFC 3329 [21]
Require option-tag	A1	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
Proxy-Require option-tag	A1	 *sec-agree*		RFC 3261 [15] RFC 3329 [21]
CSeq value method		 must be present, value not checked *SUBSCRIBE*		RFC 3261 [15]
Call-ID callid		 value not checked, but stored for later reference		RFC 3261 [15]
Max-Forwards value		 non-zero value		RFC 3261 [15]
P-Access-Network-Info access-net-spec	A1 A5 A6	 access network information and, if applicable, the cell ID access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	 Rel-15	RFC 7315 [132] RFC 7913 [154]
Accept media-range		 *application/simple-message-summary*		RFC 3261 [15] RFC 3842 [88]
Event				RFC 6665 [140]

event-type		*message-summary*		RFC 3842 [88]
Content-Length		header shall be present if UE uses TCP to send this request and if there is a message-body		RFC 3261 [15]
value		length of request body, if such is present		

Condition	Explanation
A1	IMS security (A.6a/2)
A2	GIBA (A.6a/1)
A3	Void
A4	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A5	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A6	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

A.6.2 NOTIFY for message-summary event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI		UE's contact address in SIP URI form, as provided in the Contact header within the SUBSCRIBE creating the dialog		
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15]
via-parm1:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address and protected server port of SS		
sent-by	A2	IP address and unprotected server port of SS		
via-branch		value starting with '*z9hG4bK'*		
via-parm2:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		*scscf.3gpp.org*		
via-branch		value starting with '*z9hG4bK'*		
via-parm3:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		home domain name		
via-branch		value starting with '*z9hG4bK'*		
From				RFC 3261 [15]
addr-spec		same URI as received in the To header of the previous SUBSCRIBE for message-summary event package		
tag		same value as used in the To header of the 200 response to the SUBSCRIBE for message-summary event package		
To				RFC 3261 [15]
addr-spec		same URI as received in the From header of the previous SUBSCRIBE for message-summary event package		
tag		same value as received in From tag of SUBSCRIBE for message-summary event package		
Call-ID				RFC 3261 [15]
callid		same as value received in SUBSCRIBE message		
CSeq	A1,A2			RFC 3261 [15]
value		value of CSeq sent by the SS within its previous request in the same dialog but increased by one		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec		*Contact*@home domain name		
Event	A1,A2			RFC 6665 [140]
event-type		*message-summary*		RFC 3842 [88]
Max-Forwards				RFC 3261 [15]
value		*69*		
Subscription-State				RFC 6665 [140]
substate-value		*active*		
expires		*7200*		
Content-Type				
media-type		*application/simple-message-summary*		
Content-Length				RFC 3261 [15]
value		length of message-body		
Message-body		*Messages-Waiting: no* *Message-Account:* same IMPU as in From header		RFC 3842 [88]

Condition	Explanation
A1	IMS security (A.6a/2)
A2	GIBA (A.6a/1)

A.6.3 200 OK for SUBSCRIBE for message-summary event package

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*200*		
Reason-Phrase		*OK*		
Via				RFC 3261 [15]
via-parm		same value as received in SUBSCRIBE message		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		common to-tag (subscribe msg-waiting dialog)		
From				RFC 3261 [15]
addr-spec		same value as received in SUBSCRIBE message		
tag		same value as received in SUBSCRIBE message		
Call-ID				RFC 3261 [15]
callid		same value as received in SUBSCRIBE message		
CSeq				RFC 3261 [15]
value		same value as received in SUBSCRIBE message		
Contact				RFC 3261 [15]
addr-spec		*<sip:scscf.3gpp.org>*		
Expires				RFC 3261 [15]
delta-seconds		*7200*		
Record-Route				RFC 3261 [15]
addr-spec	A1	SS P-CSCF address: protected server port of SS		
	A2	SS P-CSCF address: unprotected server port of SS (optional)		
uri-parameter		*lr*		
Content-Length				RFC 3261 [15]
value		*0*		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))

A.7 Default messages for SMS

A.7.1 MESSAGE for MT SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *MESSAGE* UE's registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message *SIP/2.0*		RFC 3261 [15] RFC 3428 [91]
Via sent-protocol sent-by via-branch		 *SIP/2.0/UDP* SS P-CSCF address: protected server port of SS value starting with '*z9hG4bK'* (NOTE 1)		RFC 3261 [15]
From addr-spec tag		 SIP URI of the IP-SM-GW any value		RFC 3261 [15]
To addr-spec tag		 default public user identity of the UE not present		RFC 3261 [15]
Call-ID callid		 a random text string generated by the SS		RFC 3261 [15]
CSeq value method		 any value *MESSAGE*		RFC 3261 [15]
Max-Forwards value		 non-zero value		RFC 3261 [15]
Accept-Contact ac-value		 *+g.3gpp.smsip;require;explicit*		RFC 3841 [64]
Request-Disposition fork-directive		 *no-fork*		RFC 3841 [64]
P-Asserted-Identity addr-spec		 SIP URI of the SS representing IP-SM-GW (same as in the From header)		RFC 3325 [89]
P-Called-Party-ID called-pty-id-spec		 same value as in the To header		RFC 7315 [132]
Content-Type media-type		 *application/vnd.3gpp.sms*		RFC 3261 [15]
Content-Length value		 length of message-body		RFC 3261 [15]
Message-body		RP-DATA message including a SMS-DELIVER TPDU equal to - TP-MTI='00'B - TP-MMS='1'B (No more messages are waiting for the MS in this SC) - TP-RP=any allowed value - TP-OA=any allowed value - TP-PID=any allowed value - TP-DCS=any allowed value - TP-SCTS=any allowed value - TP-UDL=set according to length of TP-UD field - TP-UD=a valid SMS generated by SS		TS 24.011 [92] TS 23.040 [93]

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.7.2 MESSAGE for delivery report for MT SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*MESSAGE*		RFC 3428 [91] TS 24.341 [90]
Request-URI		same P-Asserted-Identity URI as received in A.7.1		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by		not checked		
via-branch		value starting with '*z9hG4bK*'		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE		
tag		any value		
To				RFC 3261 [15]
addr-spec		same as P-Asserted-Identity URI received in A.7.1		TS 24.341 [90]
tag		not present		
Call-ID				RFC 3261 [15]
callid		any value (but different from the Call-ID values used in preceding requests of this test case)		
In-Reply-to				RFC 3261 [15]
callid		The value of the Call-Id received in the original MT SMS		
CSeq				RFC 3261 [15]
value		any value		
method		*MESSAGE*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Content-Type				RFC 3261 [15]
media-type		*application/vnd.3gpp.sms*		
Content-Length		header shall be present if UE uses TCP to send this request		RFC 3261 [15]
value		length of message-body		
Message-body		RP-ACK message		TS 24.011 [92]

A.7.3 MESSAGE for MO SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *MESSAGE* Public Service Identity of the SM-SC: value not checked Note: value as provided by the user or taking default value as defined in E.3.2.15 *SIP/2.0*		RFC 3261 [15] RFC 3428 [91]
Via sent-protocol sent-by via-branch		 *SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP) IP address or FQDN and protected server port of the UE value starting with '*z9hG4bK'*		RFC 3261 [15]
From addr-spec tag		 SIP URI of the UE any value		RFC 3261 [15]
To addr-spec tag		 same as Request-URI. not present		RFC 3261 [15]
Call-ID callid		 must be present, value not checked		RFC 3261 [15]
CSeq value method		 any value *MESSAGE*		RFC 3261 [15]
Max-Forwards value		 non-zero value		RFC 3261 [15]
P-Access-Network-Info access-net-spec	A2 A4 A5	 access network information and, if applicable, the cell ID access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	 Rel-15	RFC 7315 [132] RFC 7913 [154]
Route route-param		 <*sip:*SS P-CSCF address: protected server port of SS *;lr*>*,* *<sip:scscf.3gpp.org;lr>*		RFC 3261 [15]
Content-Type media-type		 *application/vnd.3gpp.sms*		RFC 3261 [15]
Content-Length Value		header shall be present if UE uses TCP to send this request length of message-body		RFC 3261 [15]
Message-body		RP-DATA message as specified in A.7.7 with RP-User Data set to SMS-SUBMIT type equal to - TP-MTI=' 01'B (SMS-SUBMIT) - TP-RD=any allowed value - TP-VPF=any allowed value - TP-RP=any allowed value - TP-MR=any allowed value - TP-DA=any allowed value - TP-PID=any allowed value - TP-DCS=any allowed value - TP-VP=any allowed value if TP-VPF indicates TP-VP field present; TP-VP=not present otherwise - TP-UDL=set according to length of TP-UD field - TP-UD=must be present and non-empty		TS 24.011 [92] TS 23.040 [93]

Condition	Explanation
A1	Void
A2	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A3	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A4	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A5	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

A.7.4 MESSAGE for submission report for MO SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *MESSAGE* UE's registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message *SIP/2.0*		RFC 3261 [15] RFC 3428 [91]
Via sent-protocol sent-by via-branch		 *SIP/2.0/UDP* SS P-CSCF address: protected server port of SS value starting with '*z9hG4bK'* (NOTE 1)		RFC 3261 [15]
From addr-spec Tag		 SIP URI of the IP-SM-GW any value		RFC 3261 [15]
To addr-spec tag		 default public user identity of the UE not present		RFC 3261 [15]
Call-ID Callid		 any value (but different from the Call-ID values used in preceding requests of this test case)		RFC 3261 [15]
In-Reply-to callid		 the value of the Call-Id received in the original MO SMS		RFC 3261 [15]
Cseq value method		 any value *MESSAGE*		RFC 3261 [15]
Max-Forwards Value		 non-zero value		RFC 3261 [15]
Request-Disposition fork-directive		 *fork*		RFC 3261 [15]
P-Called-Party-ID value		 same value as in the To header		RFC 3261 [15]
P-Asserted-Identity value		 Public Service Identity of the SM-SC (as received from UE in Request URI and To header in corresponding MESSAGE for MO SMS)		RFC 3325 [136]
Content-Type media-type		 *application/vnd.3gpp.sms*		RFC 3261 [15]
Content-Length value		 length of message-body		RFC 3261 [15]
Message-body		RP-ACK message with RP-User Data including SMS-SUBMIT-REPORT: TP-MTI='01'B (SMS-SUBMIT-REPORT) TP-PI='00000000'B TP-SCTS=set by the SS (encoded as specified in TS 23.040 clause 9.2.3.11)		TS 24.011 [92] TS 23.040 [93]

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.7.5 MESSAGE for status report for MO SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *MESSAGE* UE's registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message *SIP/2.0*		RFC 3261 [15] RFC 3428 [91]
Via sent-protocol sent-by via-branch		 *SIP/2.0/UDP* SS P-CSCF address: protected server port of SS value starting with '*z9hG4bK'* (NOTE 1)		RFC 3261 [15]
From addr-spec tag		 SIP URI of the IP-SM-GW any value		RFC 3261 [15]
To addr-spec tag		 default public user identity of the UE not present		RFC 3261 [15]
Call-ID callid		 any value (but different from the Call-ID values used in preceding requests of this test case)		RFC 3261 [15]
P-Asserted-Identity addr-spec		 Public Service Identity of the SM-SC (as received from UE in Request URI and To header in corresponding MESSAGE for MO SMS)		RFC 3325 [89]
CSeq value method		 CSeq value used in A.7.4 incremented by one *MESSAGE*		RFC 3261 [15]
Max-Forwards value		 non-zero value		RFC 3261 [15]
Request-Disposition fork-directive		 *no-fork*		RFC 3841 [64]
Accept-Contact ac-value		 *+g.3gpp.smsip;require;explicit*		RFC 3841 [64]
Content-Type media-type		 *application/vnd.3gpp.sms*		RFC 3261 [15]
Content-Length value		 length of message-body		RFC 3261 [15]
Message-body		RP-DATA message with RP-User Data including SMS-STATUS-REPORT TP-MTI='10'B (SMS-STATUS-REPORT) TP-MMS='0'B TP-SRQ='0'B TP-MR=same value as that set by the UE in the RP-DATA of the MO SMS TP-RA=same value as the TP-DA set by the UE in the RP-DATA of the MO SMS TP-SCTS=same value as that set by the SS in the RP-ACK acknowledging the MO SMS TP-DT=set by the SS (encoded as specified in TS 23.040 clause 9.2.3.11) TP-ST='0000000'B (Short message received by the SME)		TS 24.011 [92]

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.7.6 MESSAGE for delivery report for MO SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *MESSAGE* same as P-Asserted-Identity URI received in A.7.5 *SIP/2.0*		RFC 3261 [15] RFC 3428 [91] TS 24.341 [90]
Via sent-protocol sent-by via-branch		 *SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP) not checked value starting with '*z9hG4bK*'		RFC 3261 [15]
From addr-spec tag		 SIP URI of the UE any value		RFC 3261 [15]
To addr-spec tag		 Same as P-Asserted-Identity URI received in A.7.5 not present		RFC 3261 [15] TS 24.341 [90]
Call-ID callid		 any value (but different from the Call-ID values used in preceding requests of this test case)		RFC 3261 [15]
In-Reply-to callid		 The value of the Call-Id received in the status report for which this is a delivery report	Rel-11	RFC 3261 [15]
CSeq value method		 any value *MESSAGE*		RFC 3261 [15]
Max-Forwards value		 non-zero value		RFC 3261 [15]
Content-Type media-type		 *application/vnd.3gpp.sms*		RFC 3261 [15]
Content-Length value		header shall be present if UE uses TCP to send this request length of message-body		RFC 3261 [15]
Message-body		RP-ACK message		TS 24.011 [92]

A.7.7 RP-DATA message (UE to Network)

Information element	Value/Remark
RP-Message Type	'000'B
RP-Message Reference	Any valid value
RP-Originator Address	0 length address
RP-Destination Address	TS-Service Centre Address(default value as defined in E.3.2.14)
RP-User Data	Any valid value

A.8 Default messages for CS to PS SRVCC

A.8.1 MESSAGE UE receiving the ATGW information for CS to PS SRVCC

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*MESSAGE*		RFC 3428 [91]
Request-URI		UE's registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP*		
sent-by		SS P-CSCF address: protected server port of SS		
via-branch		value starting with '*z9hG4bK'* (NOTE 1)		
From				RFC 3261 [15]
addr-spec		*<sip:sti-sr@atcf.visited2.net>* (SIP URI of the STI-SR)		
tag		any value		
To				RFC 3261 [15]
addr-spec		default public user identity of the UE		
tag		not present		
Call-ID				RFC 3261 [15]
callid		a random text string generated by the SS		
CSeq				RFC 3261 [15]
value		any value		
method		*MESSAGE*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Accept-Contact				RFC 3841 [64]
ac-value		*+g.3gpp.smsip;require;explicit*		
Content-Disposition				RFC 3261 [15]
disp-type		*render*		
P-Asserted-Identity				RFC 3325 [89]
addr-spec		*<sip:sti-sr@atcf.visited2.net>* (SIP URI of the STI-SR)		
Content-Type				RFC 3261 [15]
media-type		*application/sdp*		
Content-Length				RFC 3261 [15]
value		length of message-body		

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

A.8.2 MESSAGE UE providing information for CS to PS SRVCC

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*MESSAGE*		RFC 3428 [91]
Request-URI		<*sip:sti-sr@atcf.visited2.net*> (same value as received in A.8.1)		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by		IP address or FQDN and protected server port of the UE		
via-branch		value starting with '*z9hG4bK'*		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE		
tag		any value		
To				RFC 3261 [15]
addr-spec		<*sip:sti-sr@atcf.visited2.net*> (SIP URI of the STI-SR) (same value as received in A.8.1)		
tag		not present		
Call-ID				RFC 3261 [15]
callid		must be present, value not checked		
CSeq				RFC 3261 [15]
value		any value		
method		*MESSAGE*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1			RFC 7315 [132] RFC 7913 [154]
access-net-spec	A3	access network information and, if applicable, the cell ID		
	A4	access network information for NR, containing access-class parameter with value "3GPP-NR" or access-type parameter with value "3GPP-NR-FDD" or "3GPP-NR-TDD", and also containing the cell ID	Rel-15	
Route				RFC 3261 [15]
route-param		<*sip*: SS P-CSCF address: protected server port of SS;*lr*>, <*sip*: *scscf.3gpp.org*;*lr*>		
Content-Type				RFC 3261 [15]
media-type		*application/sdp*		
Content-Length		header shall be present if UE uses TCP to send this request and if there is a message-body		RFC 3261 [15]
value		length of message-body		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	UE uses E-UTRAN access (A.18/1 3GPP TS 34.229-2 [5])
A4	UE uses NR access (A.18/5 3GPP TS 34.229-2 [5])

Annex B (normative): Default DHCP messages

For all the message definitions below, the acceptable order and syntax of headers and fields within these headers must be according to IETF RFCs where those headers have been defined. Typically the order of headers is not significant, but there are well defined exceptions where the order is important.

For IPv6 DHCP messages refer to RFC 3315[23].

For IPv4 DHCP messages refer to RFC 2131[55].

The contents of the messages described in the present Annex is not complete - only the fields and headers required to be checked or generated by SS are listed here. The messages sent by the UE may contain additional parameters, fields and headers which are not checked and must thus be ignored by SS.

B.1 Default DHCP messages (IPv6)

B.1.1 DHCP INFORMATION-REQUEST

Options	Value/Remarks
msg-type	INFORMATION-REQUEST (11)
transaction-id	Check If Present Note the Value to be included in Reply Message
option-code	OPTION_CLIENTID (1)
- option-len	Length of the DUID of Client
- DUID	Set to DUID of Client

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

B.1.2 DHCP REPLY

Options	Value/Remarks
msg-type	REPLY (7)
transaction-id	Set the same value as received in the corresponding Uplink Information Request message
option-code	OPTION_CLIENTID (1)
- option-len	Length of the DUID of client
- DUID	Set to DUID of Client
option-code	OPTION_SERVERID 21)
- option-len	Length of the DUID of Server
- DUID	Set to DUID of Server

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

B.1.3 DHCP SOLICIT

Options	Value/Remarks
msg-type	SOLICIT (1)
transaction-id	Check If Present Note the Value to be included in Reply Message
option-code	OPTION_CLIENTID (1)
- option-len	Length of the DUID of Client
- DUID	Set to DUID of Client
option-code	OPTION_ORO (6)
- option-len	Check Specific message contents in test case
- requested-option-code	Check Specific message contents in test case

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

B.1.4 DHCP ADVERTISE

Options	Value/Remarks
msg-type	ADVERTISE (2)
transaction-id	Set the same value as received in the corresponding Uplink solicit message
option-code	OPTION_CLIENTID (1)
- option-len	Length of the DUID of client
- DUID	Set to DUID of Client
option-code	OPTION_SERVERID (21)
- option-len	Length of the DUID of Server
- DUID	Set to DUID of Server

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

B.2 Default DHCP messages (IPv4)

B.2.1 DHCP DISCOVER

Fields	Value/Remarks
op	1 (BOOTREQUEST)
htype	Check if valid value is included
hlen	Check if valid value is included
hops	0
xid	Check For Presence Note the Value to be included in Offer Message
secs	Any Value
flags	Check For Presence Note the Value to be included in Offer Message
ciaddr	0
yiaddr	0
siaddr	0
giaddr	0
chaddr	FFS
sname	Options if indicated in sname/file else not used
file	Options if indicated in sname/file else not used
options - code - len - Type	* 53 (DHCP Message Type) 1 1 (DHCP DISCOVER)

* NOTE: Additional options may be present

B.2.2 DHCP OFFER

Fields	Value/Remarks
op	2 (BOOTREPLY)
htype	Set to SS Hardware Type
hlen	Set to SS Hardware Address Len
hops	0
xid	Set to same value as received in corresponding DISCOVER message
secs	0
flags	Set to same value as received in corresponding DISCOVER message
ciaddr	0
yiaddr	IP address of Mobile
siaddr	Set to IP address of next Boot Strap server
giaddr	Set to same value as received in corresponding DISCOVER message
chaddr	Set to same value as received in corresponding DISCOVER message
sname	Set to Server Host name
file	Set to Client Boot File Name
options	*
- code - len - Type	53 (DHCP Message Type) 1 2 (DHCP OFFER)

* NOTE: Additional options included in response to options requested by UE and supported by SS

B.2.3 DHCP INFORM

Fields	Value/Remarks
op	1 (BOOTREQUEST)
htype	Check if valid value is included
hlen	Check if valid value is included
hops	0
xid	Check For Presence Note the Value to be included in Offer Message
secs	Any Value
flags	Check For Presence Note the Value to be included in Offer Message
ciaddr	Set to UE's Network address
yiaddr	0
siaddr	0
giaddr	0
chaddr	FFS
sname	Options if indicated in sname/file else not used
file	Options if indicated in sname/file else not used
options	*
- code - len - Type	53 (DHCP Message Type) 1 8 (DHCP INFORM)

* NOTE: Additional options may be present

B.2.4 DHCP ACK

Fields	Value/Remarks
op	2 (BOOTREPLY)
htype	Set to SS Hardware Type
hlen	Set to SS Hardware Address Len
hops	0
xid	Set to same value as received in corresponding INFORM message
secs	0
flags	Set to same value as received in corresponding INFORM message
ciaddr	0
yiaddr	IP address of Mobile
siaddr	Set to IP address of next Boot Strap server
giaddr	Set to same value as received in corresponding INFORM message
chaddr	Set to same value as received in corresponding INFORM message
sname	Set to Server Host name
file	Set to Client Boot File Name
options - code - len - Type	* 53 (DHCP Message Type) 1 5 (DHCP ACK)

* NOTE: Additional options included in response to options requested by UE

Annex C (normative): Generic Test Procedure

This Annex contains information about generic test procedures.

Annex A requirements for default messages apply.

SDP structured text denoted as (name), means the "name" field must be present but any value is allowed.

C.1 Introduction

This annex specifies general procedures for IMS usages.

The annex includes also application specific procedures, e.g. for a MTSI client.

C.2 Generic Registration Test Procedure – IMS security - UMTS/EPS

The generic test procedure:

1. EPS bearer context activation according annex C.18 for UE with E-UTRA support (TS 34.229-2 A.18/1). PDP context activation according annex C.17 for UE with UTRA support (TS 34.229-2 A.18/2) only.

3. Optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.

4. The UE initiates IMS registration. SS waits for the UE to send an initial REGISTER request.

5. The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.

6. The SS waits for the UE to set up a temporary set of security associations and to send another REGISTER request, over those security associations.

7. The SS responds to the second REGISTER request with valid 200 OK response, sent over the same temporary set of security associations that the UE used for sending the REGISTER request.

8. The SS waits for the UE to send a SUBSCRIBE request over the newly established security associations.

9. The SS responds to the SUBSCRIBE request with a valid 200 OK response.

10. The SS sends a valid NOTIFY request for the subscribed registration event package.

11. The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				Annex C.17 or C.18.
2				Void.
3				Optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
4	→		REGISTER	The UE sends initial registration for IMS services.
5	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
6	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
7	←		200 OK	The SS responds with 200 OK.
8	→		SUBSCRIBE	The UE subscribes to its registration event package.
9	←		200 OK	The SS responds with 200 OK.
10	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
11	→		200 OK	The UE responds with 200 OK.

NOTE 1: The default message contents in annex A are used with conditions according to scenario and UE capabilities and, in addition,
Step 4 REGISTER uses conditions A1 and A31
Step 6 REGISTER uses conditions A2 and A31
Step 8 SUBSCRIBE uses condition A1 and A6.

NOTE 2: The procedure described in C.5 on PUBLISH requests can happen in parallel to above steps 8-11.

C.2a Generic Registration Test Procedure – GIBA - UMTS/EPS

The generic test procedure:

1 EPS bearer context activation according annex C.18 for UE with E-UTRA support (TS 34.229-2 A.18/1). PDP context activation according annex C.17 for UE with UTRA support (TS 34.229-2 A.18/2) only.

2 void

3 Optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.

4 The UE initiates IMS registration indicating support ofGIBA. SS waits for the UE to send an initial REGISTER request.

5 The SS responds to the REGISTER request with valid 200 OK response,

6 The SS waits for the UE to send a SUBSCRIBE request.

7 The SS responds to the SUBSCRIBE request with a valid 200 OK response.

8 The SS sends a valid NOTIFY request for the subscribed registration event package.

9 The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				Annex C.17 or C.18.
2				Void.
3				Optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
4	→		REGISTER	The UE sends initial registration for IMS services indicating support for GIBA procedure by not including an Authorization header field.
5	←		200 OK	The SS responds with 200 OK.
6	→		SUBSCRIBE	The UE subscribes to its registration event package.
7	←		200 OK	The SS responds with 200 OK.
8	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
9	→		200 OK	The UE responds with 200 OK.

NOTE 1: The default message contents in annex A are used.

NOTE 2: The procedure described in C.5 on PUBLISH requests can happen in parallel to steps 6-9.

C.2b Generic Registration Test Procedure – SIP digest without TLS - EPC

The generic test procedure:

1. P-CSCF statically allocated to the UE or optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
2. The UE initiates IMS registration. SS waits for the UE to send an initial REGISTER request.
3. The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.
4. The SS waits for the UE to send another REGISTER request,
5. The SS responds to the second REGISTER request with valid 200 OK response,
6. The SS waits for the UE to send a SUBSCRIBE request.
7. The SS responds to the SUBSCRIBE request with a valid 200 OK response.
8. The SS sends a valid NOTIFY request for the subscribed registration event package.
9. The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				P-CSCF statically allocated to the UE or optional, P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
2	→		REGISTER	The UE sends initial registration for IMS services. The UE should (as for TS 24.229 E.3.1.3) additionally populate the header with an Authorization header field (as defined in RFC 2617 [16], including the "username", "realm", "uri", "nonce" and "response") with a Contact header field (including the port value of an unprotected port where the UE expects to receive subsequent requests) and with the Via header field (including port value of an unprotected port where the UE expects to receive responses to the request).
3	←		401 Unauthorized	The SS responds with a 401 Unauthorized response with a WWW-Authenticate header field (containing at least one challenge applicable to the requested resource) and with the "algorithm" Authorization header field parameter set to "MD5".
4	→		REGISTER	The UE completes the security negotiation procedures sending another REGISTER request containing an Authorization header field populated as defined in Step 2, with the addition of the Authorization header field containing a challenge response, constructed using the stored “nonce” value for authentication for the same registration "cnonce", "qop", and "nonce-count" header field parameters as indicated in RFC 2617 [16].
5	←		200 OK	The SS responds with 200 OK.
6	→		SUBSCRIBE	The UE subscribes to its registration event package.
7	←		200 OK	The SS responds with 200 OK.
8	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
9	→		200 OK	The UE responds with 200 OK.

NOTE 1: The default message contents in annex A are used.

C.2c Generic Registration Test Procedure - WLAN access to EPC

The generic test procedure:

1. Steps 1-4 of TS 36.508 [94], Table 4.5A.23.3-1 are executed.
2. The UE initiates IMS registration. SS waits for the UE to send an initial REGISTER request.
3. The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.
4. The SS waits for the UE to set up a temporary set of security associations and to send another REGISTER request, over those security associations.
5. The SS responds to the second REGISTER request with valid 200 OK response, sent over the same temporary set of security associations that the UE used for sending the REGISTER request.
6. The SS waits for the UE to send a SUBSCRIBE request over the newly established security associations.

7. The SS responds to the SUBSCRIBE request with a valid 200 OK response.

8. The SS sends a valid NOTIFY request for the subscribed registration event package.

9. The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				IP-CAN bearer establishment and P-CSCF discovery
2	→		REGISTER	The UE sends initial registration for IMS services.
3	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
4	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
5	←		200 OK	The SS responds with 200 OK.
6	→		SUBSCRIBE	The UE subscribes to its registration event package.
7	←		200 OK	The SS responds with 200 OK.
8	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
9	→		200 OK	The UE responds with 200 OK.

NOTE 1: Void.

NOTE 2: The procedure described in C.5 on PUBLISH requests can happen in parallel to above steps 6-9.

Specific Message Contents

REGISTER (Step 2)

Use the default message “REGISTER” in annex A.1.1 with conditions A1 “Initial unprotected REGISTER” and A16 "IMS Registration over WLAN", in addition to any other condition due to UE capabilities.

REGISTER (Step 4)

Use the default message “REGISTER” in annex A.1.1 with conditions A2 “Subsequent REGISTER sent over security associations” and A16 "IMS Registration over WLAN", in addition to any other condition due to UE capabilities.

C.2d Void

C.3 Generic DHCP test procedure for IPv6

The generic test procedure (according to RFC 3315[23]):

1 The UE may send a DHCP SOLICIT message requesting to resolve P-CSCF Domain Name(s).

2 The SS responds with a DHCPADVERTISE message containing the IP address of the SS as P-CSCF address, if the UE requested the SIP Servers option within the DHCPSOLICIT message.

3 The UE may send a DHCP INFORMATION-REQUEST message if it has sent a DHCP SOLICIT message before. The UE shall send a DHCP INFORMATION-REQUEST if it has not sent a DHCP SOLICIT message before.

4 The SS responds with a DHCPREPLY message containing the IP address of the SS as P-CSCF address.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		DHCP SOLICIT	Optionally requesting to locate a DHCP server.
2	←		DHCPADVERTISE	Sent if the UE requested the SIP Servers option within the DHCPSOLICIT message.
3	→		DHCPINFORMATION-REQUEST	Optional message if DHCP SOLICIT was sent before, otherwise mandatory..
4	←		DHCPREPLY	Sent if DHCPINFORMATION-REQUEST is received.

NOTE: The default message contents in annex B are used.

C.4 Generic DHCP test procedure for IPv4

The generic test procedure (according to RFC 2131[55]):

1 If the UE already knows a DHCP server address, it goes to step 3. Otherwise, the UE sends a DHCPDISCOVER message locating a server.

2 The SS responds with a DHCPOFFER message.

3 The UE sends a DHCPINFORM message requesting P-CSCF address(es) in the options field.

4 The SS responds with a DHCPACK message providing the IP address of the SS as P-CSCF address.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		DHCPDISCOVER	Optionally sent if UE does not have DHCP server address.
2	←		DHCPOFFER	Sent if DHCP Discover message is received.
3	→		DHCPINFORM	Requesting P-CSCF Address(es).
4	←		DHCPACK	Including P-CSCF IP Address.

NOTE: The default message contents in annex B are used.

C.5 Default handling of PUBLISH requests

This procedure may occur within 3 seconds after a successful IMS registration.

NOTE: For sake of testability and to mitigate detrimental effect on non-IMS test cases, it is assumed that such PUBLISH request arrives at SS within 3 seconds of sending 200 OK for REGISTER.

The generic test procedure:

1 SS receives from the UE a PUBLISH request.

2 The SS responds to the PUBLISH request with a 503 Service Unavailable response carrying a Retry-after header field big enough to quench further publication traffic during test case execution.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		PUBLISH	The UE sends a PUBLISH request (A.4.3).
2	←		503 Service Unavailable	The SS responds with 503 Service Unavailable (A.4.2).

503 Service Unavailable

Use the default message “503 Service Unavailable” in annex A.4.2 with the following exceptions:

Header/param	Value/remark	Rel	Reference
Retry-after			RFC 3261 [15]
period	*7200*		
duration	Not present		
comment	Not present		

C.6 Generic Secondary PDP Context test procedure - UMTS

The generic test procedure may occur during establishment of a session. Applicable for a UE with UTRA support (TS 34.229-2 A.18/2) only.

1 The UE sends an Activate Secondary PDP Context Request message.

2 The SS responds with an Activate Secondary PDP Context Accept message.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate Secondary PDP Context Request	The UE sends a request for an additional PDP context.
2	←		Activate Secondary PDP Context Accept	The SS responds with TI flag set to ‘1’ and the TI value set to same as in step 1 in the linked TI information element.

C.7 Void

C.8 Generic test procedure for putting a MTSI speech call to hold or to resume the call from the UE - EPS

The generic test procedure for putting a MTSI speech call on hold may be performed while MTSI speech call is going on

Test procedure

1) SS waits for the UE to send an INVITE or UPDATE request with a SDP offer

2) If the UE sent an INVITE request in step 1, SS responds to the it with a 100 Trying response. No such response is sent for UPDATE.

3) SS responds to the INVITE or UPDATE request with a valid 200 OK response.

4) If the UE sent an INVITE in step 1, SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE or UPDATE	UE sends INVITE or UPDATE with a SDP offer to hold or resume the call
2	←		100 Trying	Optional: The SS responds to the INVITE with a 100 Trying provisional response
3	←		200 OK	The SS responds to INVITE or UPDATE with 200 OK to indicate that the remote UE is no more sending any media (call hold) or resumes sending media (call resume)
4	→		ACK	Optional: If the UE sent INVITE in step 1 then UE acknowledges the receipt of 200 OK for INVITE

Specific Message Contents

INVITE or UPDATE (Step 1)

Use the default message “INVITE for MO call setup” in annex A.2.1 or “UPDATE” in annex A.2.5. In case of an INVITE the UE shall use also the same URI in the request line as the SS has sent in the Contact header of an earlier message within the same dialog (in case of an UPDATE ref. to A.2.5).

The UE shall include support for precondition in the Supported header field.

The UE shall include an SDP body as described in C.21, Step 5 (respectively C.25, Step 5 for holding a video call), but with the following exceptions and clarifications:

- the sess-version number of the SDP shall be incremented by one; and
- the direction-tag for the current-status remote segment shall be "sendrecv"; and
- the UE shall either add a session level direction attribute (and remove the direction attributes of all the media lines) or modify the direction attributes of all the media lines as follows:
  - in case of Call Hold
    - If the directionality of the media lines were originally as "recvonly" then the directionality attributes within the INVITE in step 1 shall be "inactive"
    - If the directionality of the media lines were originally as "sendrecv" then the directionality attributes within the INVITE in step 1 shall be "sendonly"
  - in case of Call Resume
    - the UE shall restore the value of the directionality attributes within the SDP body their original values (the UE may use either a single session level attribute or separate attributes for each media line).

100 Trying for INVITE (Step 2) optional step used when UE sent INVITE in step 1

Use the default message "100 Trying for INVITE" in annex A.2.2.

200 OK for INVITE or UPDATE (Step 3)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	SDP body of the 200 OK response copied from the received INVITE or UPDATE but modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should send the media; and In case of Call Hold: - "sendonly" direction attribute inverted to "recvonly". Note that this applies to "a=sendonly" direction attributes only, not to the direction tags found in preconditions.

ACK (Step 4) optional step used when UE sent INVITE in step 1

Use the default message "ACK" in annex A.2.7.

C.9 Generic test procedure for putting a MTSI speech call to hold or to resume the call from the SS - EPS

The generic test procedure for putting a MTSI speech call to hold may be performed while MTSI speech call is going on

1) SS initiates the call hold by sending a re-INVITE request with an SDP offer to set the media streams into sendonly state.

2) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.

3) SS waits for the UE to respond to the INVITE request with valid 200 OK response.

4) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with a SDP offer to hold or resume the call
2	→		100 Trying	Optional: The UE responds with a 100 Trying provisional response
3	→		200 OK	The UE responds to INVITE with 200 OK to indicate that the UE is no more expecting to receive any media
4	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT call setup" in annex A.2.9 with the below exceptions. The SS uses the same URI in the request line as the UE has sent in the Contact header of the original INVITE request creating this dialog.

The SS shall include support for precondition in the Supported header field.

In case of Call Hold, the SS shall include the same lines in the SDP body as finally accepted for the MTSI call, i.e., the last SDP sent by the SS, with the following exceptions:

- version number of the SDP shall be incremented; and
- each media line shall carry direction attribute "a=sendonly".

In case of Call Resume, the SS shall include the same lines in the SDP body as sent in the message for Call Hold with the following exceptions:

- version number of the SDP shall be incremented; and
- each media line shall carry direction attribute "a=sendrecv".

100 Trying for INVITE (Step 2)

Use the default message "100 Trying for INVITE" in annex A.2.2.

200 OK for INVITE (Step 3)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	SDP answer to the SDP offer contained in the INVITE including: - All mandatory SDP lines as specified in RFC 4566[27]. - The same number of media lines ("m=") as in the INVITE. - All the media lines having directionality as "recvonly" In case of Call Hold: - All the media lines having direction attribute "a=recvonly". In case of Call Resume: - All the media lines having direction attribute "a=sendrecv".

ACK (Step 4)

Use the default message "ACK" in annex A.2.7.

C.10 Generic test procedure for MTSI conference creation - EPS

The generic test procedure for creating MTSI conference may be performed after successful IMS or early IMS registration

Test procedure

1) UE attempts to make conference call

2-7a) UE creates the voice conference. The same message sequence as in steps 2 - 8 of Annex C.21 are used to create the conference into the conference focus and negotiate the media.

8) SS responds to the INVITE request with valid 200 OK response.

9) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

10) SS waits the UE to optionally subscribe to the conference event package with a SUBSCRIBE message

11) If UE sent SUBSCRIBE, SS responds to it with 200 OK response.

12) If UE sent SUBSCRIBE, SS sends a NOTIFY for the conference event package to the UE.

13) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

Expected sequence

Step	Direction UE SS	Message	Comment
1		Make the UE attempt an IMS Conference call	
2-7a		Steps 2-8 of Annex C.21	The same messages as in steps 2 - 8 of Annex C.21
8	←	200 OK	The SS responds INVITE with 200 OK and gives the final conference URI within the response
9	→	ACK	The UE acknowledges the receipt of 200 OK for INVITE
		EXCEPTION: steps 10 – 13 describe optional behaviour depending on UE configuration. The SS shall wait up to 3s for the SUBSCRIBE of step 10	
10	→	SUBSCRIBE	UE subscribes the conference event
11	←	200 OK	SS responds to the subscription
12	←	NOTIFY	SS sends the initial state of the conference event to the UE
13	→	200 OK	UE responds to the NOTIFY

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “early IMS security” when applicable

Specific Message Contents

The specific message contents for steps 1 – 7a is otherwise identical to what have been specified in Annex C.21, but with the exceptions as below:

INVITE (Step 2)

Header/param	Value/remark
Request-Line	
Request-URI	*sip:mmtel@conf-factory* appended with px_IMS_HomeDomainName
To	
addr-spec	*sip:mmtel@conf-factory* appended with px_IMS_HomeDomainName

183 Session in Progress for INVITE (Step 4)

Header/param	Value/remark
Contact	
addr-spec	*sip:temporary@conf-factory*. appended with px_IMS_HomeDomainName
feature-param	*isfocus*
Record-Route	
rec-route	<*sip:orig@scscf.3gpp.org;lr*>, <sip:SS P-CSCF address: protected server port of SS;*lr*>

200 OK for INVITE (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Record-Route	
rec-route	Same value as in the 183 response
Contact	
addr-spec	*sip:final@conf-factory*. appended with px_IMS_HomeDomainName
feature-param	*Isfocus*

ACK (Step 9)

Use the default message "ACK" in annex A.2.7 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	*sip:final@conf-factory*. appended with px_IMS_HomeDomainName

SUBSCRIBE (Step 10)

Use the default message "SUBSCRIBE for conference event package" in annex A.5.1

200 OK (Step 11)

Use the default message "200 OK for SUBSCRIBE" in annex A.5.2

NOTIFY (Step 12)

Use the default message "MT NOTIFY for conference event package" in annex A.5.3 with condition A3

200 OK (Step 13)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

C.10a Generic test procedure for MTSI conference creation - WLAN access to EPC

The generic test procedure for creating MTSI conference may be performed after successful IMS or early IMS registration

Test procedure

1) UE attempts to make conference call.

2-3) UE creates the voice conference. The same message sequence as in steps 2 - 3 of Annex C.21a are used to create the conference into the conference focus and negotiate the media.

4-9) SS and UE complete the creation of the voice conference. The same message sequence as in steps 8-13 of Annex C.10 is used to complete the voice conference.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS Conference call	
2-3			Steps 2-3 of Annex C.21a	The same messages as in steps 2 – 3 of Annex C.21a
4-9			Steps 8-13 of Annex C.10	The same messages as in steps 8 – 13 of Annex C.10

NOTE: The default messages contents in annex A are used with condition "IMS security" or "early IMS security" when applicable

Specific Message Contents

The specific message contents for steps 2-3 is otherwise identical to what have been specified in Annex C.25a and for steps 4-9 is otherwise identical to what have been specified in Annex C.10, but with the exceptions as below:

200 OK for INVITE (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Record-Route	
rec-route	Same value as in the 180 response
Contact	
addr-spec	*sip:final@conf-factory*. appended with px_IMS_HomeDomainName
feature-param	*Isfocus*
Require	
option-tag	*precondition*
Message-body	same SDP types and values as for C.21a Step 4 (180 Ringing)

C.11 Generic test procedure for setting up MTSI MT speech call - EPS

The generic test procedure for setting up MTSI MT speech call may be performed after successful IMS or early IMS registration.

Test procedure

1) SS sends an INVITE request to the UE.
2) Void.
3) SS may receive 100 Trying from the UE.
4) SS expects and receives 183 Session Progress from the UE.
5) SS sends PRACK to the UE to acknowledge the 183 Session Progress.
6) SS expects and receives 200 OK for PRACK from the UE.
7) SS sends UPDATE to the UE, with SDP indicating that precondition is met on the server side.
8) SS expects and receives 200 OK for UPDATE from the UE, with proper SDP as answer.

9) SS may receive 180 Ringing from the UE.

10) SS may send PRACK to the UE to acknowledge the 180 Ringing.

11) SS may receive 200 OK for PRACK from the UE.

11A) The UE accepts the session invite.

12) SS expects and receives 200 OK for INVITE from the UE.

13) SS sends ACK to the UE.

14) SS sends BYE to the UE.

15) SS expects and receives 200 OK for BYE from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
4	→		183 Session Progress	The UE sends 183 response reliably with the SDP answer to the offer in INVITE
5	←		PRACK	SS acknowledges the receipt of 183 response from the UE.
6	→		200 OK	The UE responds to PRACK with 200 OK.
7	←		UPDATE	SS sends an UPDATE with SDP offer indicating SS reserved resources.
8	→		200 OK	The UE acknowledges the UPDATE with 200 OK and includes SDP answer to acknowledge its current precondition status.
9	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
11A				Make UE accept the speech AMR offer.
12	→		200 OK	The UE responds to INVITE with a 200 OK final response after the user answers the call.
13	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
14	←		BYE	The SS sends BYE to release the call.
15	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition “IMS security” or “early IMS security” when applicable

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:*(format) [Note 3, 4] Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: Void Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the AMR codec are not checked

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 4] - *s*=(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked Note 3: Parameters for the AMR codec are not checked Note 4: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

180 Ringing (Step 9)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header not present
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body 0
Message-body	Not present

C.11a Generic test procedure for MTSI MT speech call - WLAN access to EPC

The generic test procedure for setting up MT MTSI speech call may be performed after successful IMS registration over WLAN.

Test procedure

1) SS sends an INVITE request to the UE.

2) SS may receive 100 Trying from the UE.

2A) SS may receive 183 Session Progress from the UE.

2B) SS may send PRACK to the UE to acknowledge the 183 Session Progress.

2C) SS may receive 200 OK for PRACK from the UE.

3) SS may receive 180 Ringing from the UE.

4) SS may send PRACK to the UE to acknowledge the 180 Ringing Progress.

5) SS may receive 200 OK for PRACK from the UE.

5A) The UE accepts the session invite.

6) SS expects and receives 200 OK for INVITE from the UE, with optionally proper SDP as answer.

7) SS sends ACK to the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
2A	→		183 Session Progress	(Optional) The UE sends 183 response reliably with the SDP answer to the offer in INVITE
2B	←		PRACK	(Optional) SS acknowledges the receipt of 183 response from the UE.
2C	→		200 OK	(Optional) The UE responds to PRACK with 200 OK
3	→		180 Ringing	(Optional) The UE responds to the offer in INVITE with 180 Ringing with the optional SDP answer if SDP answer was not included with 183 Session Progress in step 2A
4	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
5	→		200 OK	(Optional) The UE responds to PRACK with 200 OK.
				SS waits 5 seconds for UE to send 183 Session Progress and/or 180 Ringing or none of the two before proceeding
5A				Make UE accept the speech AMR offer.
6	→		200 OK	The UE responds to INVITE with 200 OK and includes SDP answer to acknowledge its current precondition status if SDP answer was not included with 183 Session Progress in step 2A or 180 Ringing in Step 3.
7	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.

NOTE 1: Steps 3, 4, and 5 can happen in parallel to steps 2B and 2C

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:* 97 *AMR-WB/16000/1* - *a=fmtp:* 97 *mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 2A)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted.

180 Ringing (step 3)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition*
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	 length of message-body
Message-body	Optionally present only if there has been no 183 Session Progress with SDP answer at step 2A. Contents if present: Same as specified in step 2A.

200 OK (step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require	Same contents as specified in step 3.
Message-body	Present if there has been no SDP answer at step 2A or step 3. Contents if present: Same as specified in step 2A

C.11b Generic test procedure for setting up Terminating MTSI speech call - Fixed Broadband Access to EPC

The generic test procedure for setting up Terminating MTSI speech call may be performed after successful IMS registration over Fixed Broadband Access.

Test procedure

Same as described in Annex C.11

NOTE: The default messages contents in Annex A are used with condition “SIP Digest without TLS for Fixed Broadband Access” when applicable.

Expected sequence

Same as described in Annex C.11

Specific Message Content

INVITE (Step 1)

Use the default message “INVITE for MT Call” in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported	
option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 3] - *a=fmtp:*(format) [Note 3, 4] Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: Void Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the AMR codec are not checked

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 4] - *s*=(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked Note 3: Parameters for the AMR codec are not checked Note 4: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

180 Ringing (Step 9)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header not present
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body 0
Message-body	Not present

C.11c Generic test procedure for setting up Terminating MTSI speech call - Fixed Broadband Access without preconditions to EPC

The generic test procedure for setting up MTSI MT speech call over Fixed Broadband access may be performed after successful IMS registration.

Test procedure

1) SS sends an INVITE request to the UE.
2) SS may receive 100 Trying from the UE.
3) SS expects and receives 180 Ringing from the UE.
4) SS sends PRACK to the UE to acknowledge the 180 Ringing
5) SS expects and receives 200 OK for PRACK from the UE.
6) The UE accepts the session invite.
7) SS expects and receives 200 OK for INVITE from the UE.
8) SS sends ACK to the UE.
9) SS sends BYE to the UE.
10) SS expects and receives 200 OK for BYE from the UE.

Expected sequence

Step	Direction UE SS	Message	Comment
1	←	INVITE	SS sends INVITE with the first SDP offer.
2	→	100 Trying	(Optional) The UE responds with a 100 Trying provisional response
3	→	180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.(Optional) to have SDP added. If added 180 response is reliably send
4	←	PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
5	→	200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
6			Make the UE accept the speech AMR offer.
7	→	200 OK	The UE responds to INVITE with a 200 OK final response after the user answers the call. (Optional) to have SDP added. If not included in 180 response
8	←	ACK	The SS acknowledges the receipt of 200 OK for INVITE.
9	←	BYE	The SS sends BYE to release the call.
10	→	200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition “IMS security” or “early IMS security” and the condition “SIP Digest without TLS for Fixed Broadband Access” when applicable.

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240*

180 Ringing (Step 3)

Use the default message "180 Session Progress" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Message-body	The following SDP types and values shall be present. [Note 3] Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2] Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked Note 3: Parameters for the AMR codec are not checked

200 OK (Step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions when there is no SDP in 180 Ringing.

Header/param	Value/remark
Content-Type media-type	 *application/sdp* [Note 3]
Content-Length Value	 length of message-body [Note 3]
Message-body	The following SDP types and values shall be present. [Note 3] Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2] Note 1: At least one "c=" field shall be present. Note 2: Parameters for the AMR codec are not checked Note 3: These Parameters are only updated when there is no SDP in Step3 in the above call flow else default values are retained.

C.11d Generic test procedure for setting up MTSI MT speech call - UE category M1 - EPS

Test procedure:

1-15) See generic test procedure C.11.

Expected sequence:

See generic test procedure C.11.

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported	
option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:98 AMR/8000/1* - *a=fmtp:98 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked. Note 3: Parameters for the AMR codec are not checked.

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 4] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked. Note 3: Parameters for the AMR codec are not checked. Note 4: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

180 Ringing (Step 9)

See generic test procedure C.11.

C.12 Void

C.13 Generic test procedure for setting up MTSI MT text call - EPS

The generic test procedure for setting up MTSI MT text call may be performed after successful IMS or early IMS registration.

Test procedure

1) SS sends an INVITE request to the UE.

2) Void

3) SS may receive 100 Trying from the UE.

4) SS may receive 180 Ringing from the UE.

5) SS may send PRACK to the UE to acknowledge the 180 Ringing.

6) SS may receive 200 OK for PRACK from the UE.

6A) The UE accepts the session invite.
If 180 Ringing is not received from the UE after 5s from step 1, the MMI command shall be started to trigger the UE to accept the call.

7) SS receives 200 OK for INVITE from the UE.

8) SS send an ACK to acknowledge receipt of the 200 OK for INVITE

9) SS sends BYE to the UE.

10) SS expects and receives 200 Ok for BYE from the UE

Expected sequence

Step	Direction UE SS	Message	Comment
1	←	INVITE	SS sends INVITE with the first SDP offer.
2			Void
3	→	100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
4	→	180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
5	←	PRACK	(Optional) SS shall send PRACK if the 180 response contains 100rel option-tag in the Require header.
6	→	200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
6A			Make UE accept the speech AMR offer.
7	→	200 OK	The UE responds INVITE with 200 OK.
8	←	ACK	The SS acknowledges the receipt of 200 OK for INVITE.
9	←	BYE	The SS releases the call with BYE.
10	→	200 OK	The UE sends 200 OK for BYE.

NOTE: The default messages contents in annex A are used with condition “IMS security “ or “early IMS security” when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:3* Time description: - *t=0 0* Media description: - *m=text* (transport port) *RTP/AVP 102 103* - *b=AS:3* - *b=RS:0* - *b=RR:500* Attributes for media: - *a=rtpmap*:102 *t140/1000* - *a=rtpmap*:*103 red/1000* - *a=fmtp:103 99/99/99* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying for INVITE (Step 3)

Use the default message “100 Trying for INVITE” in annex A.2.2

180 Ringing (Step 4)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* [Note 3]
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	header shall be present if UE uses TCP to send this message and if there is a message body: length of message-body
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=(session name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=text* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap*:(payload type) *t140/1000* [NOTE 2] - *a=rtpmap*:(payload type) *red/1000* [NOTE 2] - *a=fmtp:*(format) [NOTE 2] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: values in fmt and values for payload type and format are not checked Note 3: Shall be present if message-body present.

200 OK for INVITE (Step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	Header not present if 180 Ringing (step 4) contained SDP. Header present if 180 Ringing (step 4) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 4 except that sess-version is incremented by one on o-line.

C.14 Void

C.15 Generic test procedure for setting up MTSI MO text call - EPS

The generic test procedure for setting up MTSI MT text call may be performed after successful IMS or early IMS registration.

Test procedure

1) Make UE initiate text.

2) UE sends an INVITE request.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with 180 Ringing response.

5) SS responds to the INVITE request with valid 200 OK response.

6) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

7) Call is released on the UE. SS waits the UE to send a BYE request.

8) SS responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				Make UE initiate the text offer.
2	→		INVITE	UE sends INVITE with a SDP offer
3	←		100 Trying	The SS responds with a 100 Trying provisional response
4	←		180 Ringing	The SS responds INVITE with 180 Ringing to indicate that the remote UE has started ringing.
5	←		200 OK	The SS responds INVITE with 200 OK
6	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
7	→		BYE	The UE releases the call with BYE
8	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition "IMS security " or "early IMS security" when applicable

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1, with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=* (protocol version) - *o=*(username) (sess-id) (sess-version) *IN IP4* or *IP6* (unicast-address for UE) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *s=*(session name) - *b=AS:* (bandwidth-value) Time description: - *t=* (time the session is active) Media description: - *m=text* (transport port) *RTP/AVP* (media format description) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap*:(payload type) *t140/1000* - *a=rtpmap*:(payload type) *red/1000* - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present.

200 OK for INVITE (Step 5)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	The following SDP types and values. The IP address on "o=" and "c=" lines and transport port on "m=" lines indicates to which IP address and port the UE should start sending the media. Use same values as received in step 2 for sess-id, sess-version, addrtype, session name, bandwidth-value (four places), media format description, payload type and format. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for SS) - *c=IN* (addrtype) (connection-address for SS) - *s=-* - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=text* (transport port) *RTP/AVP* (media format description) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap*:(payload type) *t140/1000* - *a=rtpmap*:(payload type) *red/1000* - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv*

C.16 Void

C.17 PDP context activation - UMTS

The procedure is applicable for a UE with UTRA support (TS 34.229-2 A.18/2) only.

The generic test procedure:

1 The UE sends an Activate PDP Context Request message. In the Protocol Configuration Options IE the IM CN Subsystem Signalling Flag may be set or not set, a request for P-CSCF Address or a request for DNS Server Address may be included or not.

2 The SS responds with an Activate PDP Context Accept message. In the Protocol Configuration Options IE the IM CN Subsystem Signalling Flag shall not be set, a list of P-CSCF addresses or DNS Server addresses shall only be included if a corresponding request was included in step 1.

NOTE: The required radio bearer(s) are established. For UMTS FDD they are established using RADIO BEARER SETUP (according to 3GPP TS 25.331 [58]).

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	In the Protocol Configuration Options IE the IM CN Subsystem Signalling Flag may be set or not set, a request for P-CSCF Address or a request for DNS Server Address may be included or not.
2	←		Activate PDP Context Accept	In the Protocol Configuration Options IE the IM CN Subsystem Signalling Flag shall not be set, a list of P-CSCF IP addresses or DNS Server addresses shall only be included if a corresponding request was included in step 1.

NOTE: The default message contents in annex A are used with condition “IMS AKA security “ or “GIBA” when applicable.

C.18 EPS bearer context activation - EPS

The procedure is applicable for a UE with E-UTRA support (TS 34.229-2 A.18/1) only.

The generic test procedure:

1-17 Refer to TS 36.508 [94] subclause 4.5.2.3.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-17				Registration procedure according TS 36.508 [94] subclause 4.5.2.3.

C.19 Generic test procedure for Inviting user to conference by sending a REFER request to the conference focus - EPS

The generic test procedure for Inviting user to conference by sending a REFER request to the conference focus may be performed after successful IMS or early IMS registration.

Test procedure

1) UE invites a user to the conference created. SS waits the UE to send to the conference focus a REFER request, which refers to the user to be invited to the conference.

2) SS responds to the REFER request with a valid 202 Accepted response.

3) SS sends an initial NOTIFY to tell that the invited user is trying to join the conference.

4) UE responds to the NOTIFY request with valid 200 OK response.

5) SS sends the final NOTIFY to tell that the invited user has successfully joined the conference.

6) UE responds to the NOTIFY request with a valid 200 OK response.

7) Optional: If UE subscribed the conference event package during the generic test procedure of Annex C.10, SS sends a NOTIFY for the conference event package to the UE to notify that the user joined the conference.

8) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REFER	UE sends REFER to SS referring to the conference
2	←		202 Accepted	The SS responds with a 202 final response
3	←		NOTIFY	The SS sends initial NOTIFY for the implicit subscription created by the REFER request
4	→		200 OK	The UE responds the NOTIFY with 200 OK
5	←		NOTIFY	The SS sends a NOTIFY related to REFER request to confirm that the invited user was able to join the conference
6	→		200 OK	The UE responds the NOTIFY with 200 OK
7	←		NOTIFY	Optional: If the UE has subscribed the conference event package, the SS sends a NOTIFY for conference event package to inform that the invited user was able to join the conference
8	→		200 OK	Optional: The UE responds the NOTIFY with 200 OK

Specific Message Contents

REFER (Step 1)

Use the default message “MO REFER” in annex A.2.10 with the following exceptions:

Header/param	Value/remark
Request-URI	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
Refer-To	
addr-spec	SIP URI or tel URI of the user invited to the conference. If an active session exists, the Replaces header in the header portion of the SIP URI shall be included (mandatory inclusion is stated in IR.92 [133]) and set to the dialog ID of the active session according to RFC 3891. In this case, if the user has been invited with a tel URI, the UE shall convert the tel URI to a SIP URI according to RFC 3261 [15] clause 19.1.6. (NOTE: the dialog ID is percent encoded according to RFC 3986).
To	
addr-spec	remote SIP URI as used in To header in step 2 of C.10
tag	remote tag of the dialog with the conference focus created in step 2 of C.10
Route	
route-param	URIs of the Record-Route header of 183 response sent in step 4 of C.10 in reverse order

NOTIFY (Step 3)

Use the default message “MT NOTIFY for refer package” in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

NOTIFY (Step 5)

Use the default message “MT NOTIFY for refer package” in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

NOTIFY (Step 7)

Use the default message “NOTIFY for conference event package” in annex A.5.3 with the following exceptions:

Header/param	Value/remark
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<conference-info xmlns="urn:ietf:params:xml:ns:conference-info"* *entity="sip:final@conf-factory.* appended with px_IMS_HomeDomainName*"* *state="partial"* *version="* value as in previous notification for conference event package but incremented by one*"* *<users>* *<user entity="* **SIP URI or tel URI of the invited user***">* *<endpoint entity="* **Contact URI of the invited user***">* *<status>connected</status>* *<joining-method>dialed-in</joining-method>* *<media id="1">* *<type>audio</type>* *<label>* **unique identifier for the media stream between the focus and the endpoint of the invited user (e.g. 11223)***</label>* *<src-id>***random SSRC value***</src-id>* *<status>sendrecv</status>* *</media>* *</endpoint>* *</users>* *</conference-info>*

C.20 Generic Test Procedure for IMS emergency registration - EPS

Test procedure:

1) SS waits for the UE to send an initial REGISTER request.

2) The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.

3) The SS waits for the UE to set up a temporary set of security associations and to send another REGISTER request over those security associations.

4) The SS responds to the second REGISTER request with valid 200 OK response, sent over the same temporary set of security associations that the UE used for sending the REGISTER request.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The UE sends initial IMS emergency registration
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
3	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The SS responds with 200 OK.

Specific Message Contents:

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1 with conditions A1 and A7 .

The contents of From and To headers of the REGISTER request shall be according to condition A7.

REGISTER (Step 3)

Use the default message “REGISTER” in annex A.1.1 with conditions A2 A7, and A31.

The contents of From and To headers of the REGISTER request shall be according to condition A7.

200 OK for REGISTER (Step 4)

Use the default message “200 OK for REGISTER” in annex A.1.3 with conditions A3 and A21.

C.20a Void

C.21 Generic test procedure for setting up MTSI MO speech call - EPS

Test procedure:

1) MO speech is initiated on the UE. The call is initiated towards the URI configured to SS as px_IMS_CalleeUri. Depending on the UE support this URI may be either SIP or Tel URI, possibly containing a dialstring indicating a global, home local or geo-local telephone number. SS waits the UE to send an INVITE request with first SDP offer

2) UE sends an INVITE request to the SS.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with a 183 Session Progress response.

5) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

6) SS responds to the PRACK request with a 200 OK.

7) SS waits for the UE to send a UPDATE request containing the final SDP offer.

8) SS responds to the UPDATE request with a 200 OK.

9) SS responds to the INVITE request with a 180 Ringing.

10) SS waits for the UE to send a PRACK request.

11) SS responds to the PRACK request with a 200 OK.

12) SS responds to the INVITE request with a 200 OK.

13) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS speech call	
2	→		INVITE	UE sends INVITE with the first SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		183 Session Progress	SS sends an SDP answer.
5	→		PRACK	UE acknowledges and optionally offers a second SDP if a dedicated EPS bearer is established by the network.
6	←		200 OK	SS sends a 200 OK and answers the second SDP if present.
7	→		UPDATE	Optional step: UE sends a second SDP if a dedicated EPS bearer is established by the network.
8	←		200 OK	Optional step: SS sends a 200 OK.
9	←		180 Ringing	SS sends a 180 Ringing.
10	→		PRACK	UE acknowledges.
11	←		200 OK	SS responds PRACK with 200 OK.
12	←		200 OK	SS responds INVITE with 200 OK.
13	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message “INVITE for MO Call” in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 7] - *b=RR:* (bandwidth-value) [Note 7] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 8] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 9, 10] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=rtpmap:* (payload type) *AMR/8000* [Note 8] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 9, 10] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=fmtp:* (format) - *a=ecn-capable-rtp: leap ect=0* [Note 3] - *a=rtcp-fb:* nack ecn* [Note 3] - *a=rtcp-xr:ecn-sum* [Note 3] - *a=rtcp-rsize* [Note 3] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 4] - *a=crypto:1* *AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20* | *1:4FEC_ORDER=FEC_SRTP"* [Note 4] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: Void. Note 3: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 4: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 5: Void. Note 6: Void. Note 7: The RR value must be greater than 0. The RS value can be any value. Note 8: The AMR channel number shall be "/1" or omitted. Note 9: The max-red values from 0 to 220 are allowed. Note 10: The parameters mode-set, mode-change-period, mode-change-neighbor, crc, robust-sorting and interleaving shall not be included.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:3*7 - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 3] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 3] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2. Note 6: Void

PRACK (Step 5)

Use the default message “PRACK” in annex A.2.4 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] [Note 5] - *a=fmtp:* (format) [Note 3, 4] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one. Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the AMR codec are not checked Note 5: The AMR channel number shall be “/1” or omitted.

200 OK for PRACK (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 OK response copied from the received PRACK and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

UPDATE (Step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Require	Same contents as specified in step 5.
Message-body	Same contents as specified in step 5.

200 OK for UPDATE (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

180 Ringing (Step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6 applying condition A3 (Response sent reliably).

C.21a Generic test procedure for MTSI MO speech call – WLAN access to EPC

Test procedure:

1) MO speech is initiated on the UE. The call is initiated towards the URI configured to SS as px_IMS_CalleeUri. Depending on the UE support this URI may be either SIP or Tel URI, possibly containing a dialstring indicating a global, home local or geo-local telephone number. SS wait for the UE to send an INVITE request with first SDP offer.

2) UE sends an INVITE request to the SS.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with a 180 Ringing response.

5) SS waits for the UE to send a PRACK request.

6) SS responds to the PRACK request with a 200 OK.

7) SS responds to the INVITE request with a 200 OK.

8) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS speech call	
2	→		INVITE	UE sends INVITE with the first SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		180 Ringing	SS sends Ringing with an SDP answer.
5	→		PRACK	UE acknowledges.
6	←		200 OK	SS sends a 200 OK response for PRACK.
7	←		200 OK	SS sends a 200 OK for INVITE.
8	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message “INVITE for MO Call” in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 4] - *b=RR:* (bandwidth-value) [Note 4] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:* (format) *mode-change-capability=2; max-red*=(att-field) [Note 3, 5] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=rtpmap:* (payload type) *AMR/8000* [Note 2] - *a=fmtp:* (format) *mode-change-capability=2; max-red*=(att-field) [Note 3, 5] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=fmtp:* (format) - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted. Note 3: The max-red values from 0 to 220 are allowed. Note 4: The RR value must be greater than 0. The RS value can be any value. Note 5: The parameters mode-set, mode-change-period, mode-change-neighbor, crc, robust-sorting and interleaving shall not be included.

180 Ringing (Step 4)

Use the default message "180 Ringing" in annex A.2.6 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 2] - *b=AS:* 37 - *b=RS:* (bandwidth-value) [Note 3] - *b=RR:* (bandwidth-value) [Note 3] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Transport port is the port number of the SS (see RFC 3264 clause 6). Note 3: The bandwidth-value is copied from step 2.

C.21b Generic test procedure for Originating MTSI Voice Call - Fixed Broadband Access to EPC

Test procedure:

Same as described in C.21

Expected sequence:

Same as described in Annex C.21

Specific Message Contents

INVITE (Step 2)

Editor's note: whether UE sends as attributes for preconditions "a=curr:qos local sendrecv" or "a=curr:qos local none" needs to be finalized.

Use the default message "INVITE for Originating Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 7] - *b=RR:* (bandwidth-value) [Note 7] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 8] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 9] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=fmtp:* (format) - *a=ecn-capable-rtp: leap ect=0* [Note 3] - *a=rtcp-fb:* nack ecn* [Note 3] - *a=rtcp-xr:ecn-sum* [Note 3] - *a=rtcp-rsize* [Note 3] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: Void. Note 3: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 4: Void. Note 5: Void Note 6: Void Note 7: The RR value must be greater than 0. The RS value can be any value. Note 8: The AMR channel number shall be "/1" or omitted. Note 9: Values from 0 to 220 are allowed

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:3*7 - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Void. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2. Note 6: Void

PRACK (Step 5)

Use the default message “PRACK” in annex A.2.4 with the following exceptions:

Header/param	Value/Remark
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) - *a=fmtp:* (format) [Note 3, 4] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one. Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the AMR and other applicable codec are not checked

200 OK for PRACK (Step 6)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 OK response copied from the received PRACK and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

UPDATE (Step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Message-body	Same contents as specified in step 5.

200 OK for UPDATE (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

180 Ringing (Step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6 applying condition A3 (Response sent reliably).

C.21c Generic test procedure for Originating MTSI Voice Call - Fixed Broadband Access without preconditions to EPC

Test procedure:

Same as described in Annex C.21a

Expected sequence:

Same as described in Annex C.21a

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for Originating Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 6] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 7] - *a=rtpmap:* (payload type) *telephone-event* [Note 4] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=rtcp-rsize* [Note 2] - *a=ptime:20* - *a=maxptime:240* Note 1: At least one "c=" field shall be present. Note 2: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 3: Void. Note 4: a rate may be added to the "telephone-event" separated by "/" (e.g. "telephone-event/8000") Note 5: The RR value must be greater than 0. The RS value can be any value. Note 6: The AMR channel number shall be "/1" or omitted. Note 7: Values from 0 to 220 are allowed

180 Ringing (Step 4)

Use the default message "180 Ringing" in annex A.2.6 with the following exceptions:

Header/param	Value/Remark
Content-Type **media-type**	*application/sdp*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:3*7 - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* - *a=sendrecv* Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Void. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2.

C.21d Generic test procedure for MTSI MO speech call - UE category M1 - EPS

Test procedure:

1- 13) See generic test procedure C.21.

Expected sequence:

See generic test procedure C.21.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 2] - *b=RR:* (bandwidth-value) [Note 2] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 4, 5] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The RR value must be greater than 0. The RS value can be any value. Note 3: The AMR channel number shall be "/1" or omitted. Note 4: The max-red values from 0 to 220 are allowed. Note 5: The parameters mode-set, mode-change-period, mode-change-neighbor, crc, robust-sorting and interleaving shall not be included.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 2] - *b=AS:3*7 - *b=RS:* (bandwidth-value) [Note 3] - *b=RR:* (bandwidth-value) [Note 3] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* - *a=inactive* [Note 4] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: transport port is the port number of the SS (see RFC 3264 clause 6). Note 3: The bandwidth-value is copied from step 2. Note 4: The attribute a=inactive shall be present if it was included in step 2.

PRACK (Step 5)

Use the default message “PRACK” in annex A.2.4 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 3, 5] - *a=fmtp:* (format) [Note 3, 4] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one. Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the AMR codec are not checked Note 5: The AMR channel number shall be “/1” or omitted.

200 OK for PRACK (Step 6)

See generic test procedure C.21.

UPDATE (Step 7)

See generic test procedure C.21.

200 OK for UPDATE (Step 8)

See generic test procedure C.21.

180 Ringing (Step 9)

See generic test procedure C.21.

C.21e Void

C.21f Generic test procedure for setting up MTSI MO speech call without preconditions - EPS

Test procedure:

1) MO speech is initiated on the UE without preconditions. The call is initiated towards the URI configured to SS as px_IMS_CalleeUri. Depending on the UE support this URI may be either SIP or Tel URI, possibly containing a dialstring indicating a global, home local or geo-local telephone number. SS waits the UE to send an INVITE request with first SDP offer

2) UE sends an INVITE request to the SS.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with a 183 Session Progress response.

5) SS waits for the UE to send a PRACK request.

6) SS responds to the PRACK request with a 200 OK.

7) SS responds to the INVITE request with a 180 Ringing.

8) SS responds to the INVITE request with a 200 OK.

9) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS speech call	
2	→		INVITE	UE sends INVITE with the first SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		183 Session Progress	SS sends an SDP answer.
5	→		PRACK	UE acknowledges with PRACK.
6	←		200 OK	SS sends a 200 OK.
7	←		180 Ringing	SS sends a 180 Ringing.
8	←		200 OK	SS responds INVITE with 200 OK.
9	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with the following exceptions:

Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 4] - *b=RR:* (bandwidth-value) [Note 4] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 5] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 6, 7] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=rtpmap:* (payload type) *AMR/8000* [Note 5] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 6, 7] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=fmtp:* (format) - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=rtcp-rsize* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 3] - *a=crypto:1* *AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20|1:4FEC_ORDER=FEC_SRTP"* [Note 3] Note 1: At least one "c=" field shall be present. Note 2: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: The RR value must be greater than 0. The RS value can be any value. Note 5: The AMR channel number shall be "/1" or omitted. Note 6: The max-red values from 0 to 220 are allowed. Note 7: The parameters mode-set, mode-change-period, mode-change-neighbor, crc, robust-sorting and interleaving shall not be included.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:3*7 - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 3] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 3] Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2.

180 Ringing (Step 7)

Use the default message “180 Ringing for INVITE” in annex A.2.6 applying condition A1 (in addition to any other applicable conditions).

C.21g Generic test procedure for setting up MTSI MO speech call - EPS fallback

Expected sequence:

Step	Direction UE	Direction SS	Message	Comment
1	→		INVITE	UE sends INVITE with the first SDP offer.
2	←		100 Trying	SS sends a 100 Trying provisional response.
3	←		183 Session Progress	SS sends an SDP answer.
4	→		PRACK	UE acknowledges reception of 183 Session Progress.
5	←		200 OK	SS sends a 200 OK response for PRACK.
6	→		UPDATE	UE sends an UPDATE request containing a second SDP offer
7	←		200 OK	SS sends a 200 OK response for UPDATE containing an SDP answer.
8	←		180 Ringing	SS sends a 180 Ringing.
9	←		200 OK	SS responds to INVITE with 200 OK.
10	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MO Call" in annex A.2.1 applying conditions A1, A3, A4 and A28 (in addition to any other applicable conditions) and with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 2] - *b=RR:* (bandwidth-value) [Note 2] Attributes for media: - *a=rtpmap:* (payload type) *EVS/16000* [Note 3] - *a=fmtp:* (format) *max-red*= (att-field) [Note 4, 5] - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 4, 6] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 4, 6] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=fmtp:* (format) - *a=ecn-capable-rtp: leap ect=0* [Note 7] - *a=rtcp-fb:* nack ecn* [Note 7] - *a=rtcp-xr:ecn-sum* [Note 7] - *a=rtcp-rsize* [Note 7] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 8] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20|1:4FEC_ORDER=FEC_SRTP"* [Note 8] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The RR value must be greater than 0. The RS value can be any value. Note 3: The channel number shall be “/1” or omitted. Note 4: The max-red values from 0 to 220 are allowed. Note 5: The parameters dtx, dtx-recv and evs-mode-switch shall not be present. Note 6: The parameters mode-set, mode-change-period, mode-change-neighbor, crc, robust-sorting and interleaving shall not be included. Note 7: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 8: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE.

100 Trying (Step 2)

Use the default message “100 Trying for INVITE” in annex A.2.2 applying condition A1.

183 Session Progress (Step 3)

Use the default message "183 Session Progress" in annex A.2.3 applying condition A1 (in addition to any other applicable conditions) and with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:65* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 2] - *b=AS:65* - *b=RS:* (bandwidth-value) [Note 3] - *b=RR:* (bandwidth-value) [Note 3] Attributes for media: - *a=rtpmap:* (payload type) *EVS/16000/1* [Note 1] - *a=fmtp:* (format) *max-red=220* [Note 1, 4, 5] - *a=ecn-capable-rtp: leap ect=0* [Note 6] - *a=rtcp-fb:* nack ecn* [Note 6] - *a=rtcp-xr:ecn-sum* [Note 6] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 7] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 7] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The values for fmt, payload type and format are copied from step 2. Note 2: Transport port is the port number of the SS (see RFC 3264 clause 6). Note 3: The bandwidth-value is copied from step 2. Note 4: All present br, br-send and br-recv parameter=value pairs are copied from step 2. Note 5: bw, bw-send and bw-recv parameter are copied from bw at step 2. Note 6: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 7: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE.

PRACK (Step 4)

Use the default message “PRACK” in annex A.2.4 applying conditions A1 and A7.

200 OK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 applying conditions A1, A10 and A22 (in addition to any other applicable conditions).

UPDATE (Step 6)

Use the default message "PRACK" in annex A.2.4 applying conditions A1 and A7 (in addition to any other applicable conditions) and with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] [Note 5] - *a=fmtp:* (format) [Note 3][Note 4] - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the codec are not checked Note 5: The channel number shall be "/1" or omitted.

200 OK for UPDATE (Step 7)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 applying conditions A1, A10 and A21 (in addition to any other applicable conditions) and with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length Value	 length of message-body
Message-body	SDP body of the 200 OK response copied from the received UPDATE request and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

180 Ringing (Step 8)

Use the default message “180 Ringing for INVITE” in annex A.2.6 applying conditions A1 and A13 (in addition to any other applicable conditions).

200 OK (Step 9)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 applying conditions A1, A19 and A21 (in addition to any other applicable conditions).

ACK (Step 10)

Use the default message “180 Ringing for INVITE” in annex A.2.6 applying condition A1.

C.22 Generic test procedure for setting up emergency speech call - EPS

Test procedure:

1) SS waits for UE to send an INVITE request.
2) The SS responds to the INVITE request with a 100 Trying response.
3) SS responds to the INVITE request with a 180 Ringing response.
4) The SS responds to the INVITE request with a 200 OK response.
5) The SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with the first SDP offer.
2	←		100 Trying	SS sends a 100 Trying provisional response.
3	←		180 Ringing	SS sends a 180 Ringing.
4	←		200 OK	SS responds INVITE with 200 OK.
5	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MO Call" in annex A.2.1 with condition A27 and the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec (AMR/8000 and/or AMR-WB/16000) shall be present in the media attributes, optionally including channel number "/1".

180 Ringing for INVITE (Step 3)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with conditions A4 and A13.

200 OK for INVITE (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with conditions A6and A21 and the following exceptions:

Header/param	Value/remark
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1] - *b=AS:37* - *b=RS:0* - *b=RR:0* Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000/1 or AMR-WB/16000/1* [Note 1] [Note2] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Note 1: The value for fmt, payload type and format is copied from step 1. Note 2: If UE included AMR-WB/16000 in step 1, SS uses AMR-WB/16000/1. Otherwise SS uses AMR/8000/1.

C.22a Void

Void

C.23 Procedure to register another IMPU over existing SAs

The generic test procedure:

1 The UE initiates IMS registration for the new IMPU. SS waits for the UE to send an initial REGISTER request over the existing set of IPSec SAs.

2 The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.

3 The SS waits for the UE to send another REGISTER request, over the existing security associations.

4 The SS responds to the second REGISTER request with valid 200 OK response

5 The SS sends a NOTIFY request for the registration event package.

6 The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The UE sends initial registration for the new IMPU over the existing IPSec SAs
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge
3	→		REGISTER	The UE sends another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The SS responds with 200 OK.
5	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing partial registration state information for the newly registered public user identity in the XML body
6	→		200 OK	The UE responds with 200 OK.

NOTE: The default message contents in annex A are used apart from the XML body in step 5. The body shall be specified within the test case referring to this procedure.

C.24 Generic test procedure for SRVCC media removal

Test procedure:

1) UE sends an re-INVITE request to the SS.

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with a 200 OK.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with audio removed.
2	←		100 Trying	SS sends a 100 Trying provisional response.
3	←		200 OK	SS responds INVITE with 200 OK.
4	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MO Call" in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Request-Line	
Method	*INVITE*
Request-URI	Same value as the URI from the Contact header of the original INVITE request as sent by SS
SIP-Version	*SIP/2.0*
Message-body	The following SDP types and values. Session description: - v=0 - o=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - s=(session name) - c=IN (addrtype) (connection-address for UE) [Note 1] - b=AS: (bandwidth-value) Time description: - t= (start-time) (stop-time) Media description: - m=audio 0 RTP/AVP (fmt) - c=IN (addrtype) (connection-address for UE) [Note 1] Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one

200 OK (Step 3)

Use the default message "200 OK" in annex A.3.1 with the following exceptions:

Header/param	Value/Remark
Contact addr-spec	 Same value as the URI from the Contact header of the original INVITE request as sent by SS
Content-Type media-type	*application/sdp*
Content-Length value	 length of message-body
Message Body	The following SDP types and values: Session description: - v=0 - *o*=- *1111111111* (sess-version) *IN* (addrtype) (unicast-address for SS) [Note 2] - *s*=- - c=IN (addrtype) (connection-address for SS) - *b*=*AS*:37 Time description: - *t=0 0* Media description: - m=audio 0 RTP/AVP (fmt) [Note 3] Note 1: Void. Note 2: sess-version incremented by one if SDP changed compared to last SDP sent by SS Note 3: The value for fmt is copied from step 1

ACK (Step 4)

Use the default message "ACK" in annex A.2.7 with condition A5 and the following exceptions:

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 ACK Same value as the URI from the Contact header of the original INVITE request as sent by SS SIP/2.0		RFC 3261 [15]
To addr-spec tag		 Same value as used in the INVITE of step 1 Same value as used in the INIVTE of step 1		RFC 3261 [15]

NOTE 1: when A.2.7 refers to "INVITE", the re-INVITE of step 1 is meant.

C.25 Generic test procedure for setting up MTSI MO video call - EPS

Test procedure:

1) MO video call is initiated on the UE. The call is initiated towards the URI configured to SS as px_IMS_CalleeUri. Depending on the UE support this URI may be either SIP or Tel URI, possibly containing a dialstring indicating a global, home local or geo-local telephone number. SS waits the UE to send an INVITE request with first SDP offer

2) UE sends an INVITE request to the SS.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with a 183 Session Progress response

5) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

6) SS responds to the PRACK request with a 200 OK.

7) SS waits for the UE to send a UPDATE request containing the final SDP offer.

8) SS responds to the UPDATE request with a 200 OK.

9) SS responds to the INVITE request with a 180 Ringing.

10) SS waits for the UE to send a PRACK request.

11) SS responds to the PRACK request with a 200 OK.

12) SS responds to the INVITE request with a 200 OK.

13) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction UE SS	Message	Comment
1		Make the UE attempt an IMS video call	
2	→	INVITE	UE sends INVITE with the first SDP offer.
3	←	100 Trying	SS sends a 100 Trying provisional response.
4	←	183 Session Progress	SS sends an SDP answer.
5	→	PRACK	UE acknowledges and optionally offer a second SDP if a dedicated EPS bearer is established by the network.
6	←	200 OK	SS sends a 200 OK and answers the second SDP if present.
7	→	UPDATE	Optional step: UE sends a second SDP if a dedicated EPS bearer is established by the network.
8	←	200 OK	Optional step: SS sends a 200 OK.
9	←	180 Ringing	SS sends a 180 Ringing.
10	→	PRACK	UE acknowledges.
11	←	200 OK	SS responds PRACK with 200 OK.
12	←	200 OK	SS responds INVITE with 200 OK.
13	→	ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 4] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 4] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=fmtp:* (format) - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 2] - *a=pcfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id*= (att-field) Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The tcap/pcfg attributes are present if RTP/AVP is present on the m line. Note 3: The AMR channel number shall be “/1” or omitted. Note 4: Values from 0 to 220 are allowed

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=acfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* [Note 1] - *a=fmtp:* (format) (format specific parameters) [Note 1] - *a=inactive* [Note 4] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, bandwidth, payload type, format and format specific parameters copied from step 2. Note 2: Present if tcap/pcfg attributes were included in step 2. Note 3: Void

PRACK (Step 5)

Use the default message “PRACK” in annex A.2.4 with the exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id=* (att-field) - *a=sendrecv* [Note 4] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one. Note 3: The AMR channel number shall be “/1” or omitted.

200 OK for PRACK (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 response copied from the received PRACK and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: - *a=curr:qos remote sendrecv*

UPDATE (Step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Require	Same contents as specified in step 5.
Message-body	Same contents as specified in step 5.

200 OK for UPDATE (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: *- a=curr:qos remote sendrecv*

C.25a Generic test procedure for MTSI MO video call - WLAN access to EPC

Test procedure:

1) MO video call is initiated on the UE. The call is initiated towards the URI configured to SS as px_IMS_CalleeUri. Depending on the UE support this URI may be either SIP or Tel URI, possibly containing a dialstring indicating a global, home local or geo-local telephone number. SS waits for the UE to send an INVITE request with first SDP offer.
2) UE sends an INVITE request to the SS.
3) SS responds to the INVITE request with a 100 Trying response.
4) SS responds to the INVITE request with a 180 Ringing response.
5) SS waits for the UE to send a PRACK request.
6) SS responds to the PRACK request with a 200 OK response.
7) SS responds to the INVITE request with a 200 OK response.
8) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK response for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS video call	
2	→		INVITE	UE sends INVITE with the first SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		180 Ringing	SS sends Ringing with an SDP answer.
5	→		PRACK	UE acknowledges
6	←		200 OK	SS sends a 200 OK response for PRACK
7	←		200 OK	SS sends a 200 OK for INVITE.
8	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with the following exceptions:

<table>
<tr><th>Header/param</th><th>Value/Remark</th></tr>
<tr><td>Supported
option-tag</td><td>
precondition</td></tr>
<tr><td>Message-body</td><td>The following SDP types and values.

Session description:
- v=0
- o=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE)
- s=(session name)
- c=IN (addrtype) (connection-address for UE) [Note 1]
- b=AS: (bandwidth-value)

Time description:
- t= (start-time) (stop-time)

Media description:
- m=audio (transport port) RTP/AVP (fmt)
- c=IN (addrtype) (connection-address for UE) [Note 1]
- b=AS: (bandwidth-value)
- b=RS: (bandwidth-value)
- b=RR: (bandwidth-value)

Attributes for media:
- a=rtpmap: (payload type) AMR-WB/16000 [Note 3]
- a=fmtp: (format) mode-change-capability=2; max-red=(att-field) [Note 4]
- a=rtpmap: (payload type) telephone-event/16000
- a=fmtp: (format)
- a=rtpmap: (payload type) AMR/8000 [Note 3]
- a=fmtp: (format) mode-change-capability=2; max-red=(att-field) [Note 4]
- a=rtpmap: (payload type) telephone-event/8000- a=fmtp: (format)
- a=ptime:20
- a=maxptime:240

Attributes for preconditions:
- a=curr:qos local sendrecv
- a=curr:qos remote none
- a=des:qos mandatory local sendrecv
- a=des:qos optional remote sendrecv

Media description:
- m=video (transport port) RTP/AVPF (fmt) or RTP/AVP (fmt) [Note 2]
- c=IN (addrtype) (connection-address for UE) [Note 1]
- b=AS: (bandwidth-value)
- b=RS: (bandwidth-value)
- b=RR: (bandwidth-value)

Attributes for media:
- a=tcap:1 RTP/AVPF [Note 2]
- a=pcfg:1 t=1 [Note 2]
- a=rtpmap: (payload type) H264/90000
- a=fmtp: (format) profile-level-id= (att-field)

Attributes for preconditions:
- a=curr:qos local sendrecv
- a=curr:qos remote none
- a=des:qos mandatory local sendrecv
- a=des:qos optional remote sendrecv

Note 1: At least one "c=" field shall be present.
Note 2: The tcap/pcfg attributes are present if RTP/AVP is present on the m line.
Note 3: The AMR channel number shall be "/1" or omitted.
Note 4: Values from 0 to 220 are allowed.</td></tr>
</table>

180 Ringing (Step 4)

Use the default message "180 Ringing" in annex A.2.6 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:* (bandwidth-value) [Note 1] Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=acfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* [Note 1] - *a=fmtp:* (format) (format specific parameters) [Note 1] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: The value for fmt, bandwidth, payload type, format and format specific parameters copied from step 2. Note 2: Present if tcap/pcfg attributes were included in step 2. Note 3: The AMR channel number shall be “/1” or omitted.

C.25b Generic test procedure for Originating MTSI Video Call - Fixed Broadband Access to EPC

Test procedure:

Same as described in Annex C.25a

Expected sequence:

Same as described in Annex C.25a

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for Originating Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 4] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=fmtp:* (format) - *a=ptime:20* - *a=maxptime:240* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 2] - *a=pcfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id*= (att-field) Note 1: At least one "c=" field shall be present. Note 2: The tcap/pcfg attributes are present if RTP/AVP is present on the m line. Note 3: The AMR channel number shall be "/1" or omitted. Note 4: Values from 0 to 220 are allowed.

180 Ringing (Step 4)

Use the default message "180 Ringing" in annex A.2.6 with the following exceptions:

Header/param	Value/Remark
Content-Type **media-type**	 *application/sdp*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a= acfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) (format specific parameters) [Note 1] Note 1: The value for fmt, bandwidth, payload type and format specific parameters copied from step 2. Note 2: Present if tcap/pcfg attributes were included in step 2 Note 3: Void

C.26 Generic test procedure for setting up MTSI MT video call - EPS

Test procedure

1) SS sends an INVITE request to the UE.

2) Void

3) SS may receive 100 Trying from the UE.

4) SS expects and receives 183 Session Progress from the UE.

5) SS sends PRACK to the UE to acknowledge the 183 Session Progress.

6) SS expects and receives 200 OK for PRACK from the UE.

7) SS sends UPDATE to the UE, with SDP indicating that precondition is met on the server side.

8) SS expects and receives 200 OK for UPDATE from the UE, with proper SDP as answer.

9) SS may receive 180 Ringing from the UE.

10) SS may send PRACK to the UE to acknowledge the 180 Ringing.

11) SS may receive 200 OK for PRACK from the UE.

11A) The UE accepts the session invite.

12) SS expects and receives 200 OK for INVITE from the UE.

13) SS sends ACK to the UE.

14) SS sends BYE to the UE.

15) SS expects and receives 200 OK for BYE from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
4	→		183 Session Progress	The UE sends 183 response reliably with the SDP answer to the offer in INVITE
5	←		PRACK	SS acknowledges the receipt of 183 response from the UE.
6	→		200 OK	The UE responds to PRACK with 200 OK.
7	←		UPDATE	SS sends an UPDATE with SDP offer indicating SS reserved resources.
8	→		200 OK	The UE acknowledges the UPDATE with 200 OK and includes SDP answer to acknowledge its current precondition status.
9	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
11A				Make UE accept the video offer.
12	→		200 OK	The UE responds to INVITE with a 200 OK final response after the user answers the call.
13	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
14	←		BYE	The SS sends BYE to release the call.
15	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “early IMS security” when applicable

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:352* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Media description: - *m=video (transport port) RTP/AVPF 101* - *b=AS: 315* - *b=RS: 0* - *b=RR: 2500* Attributes for media: - *a=rtpmap: 101 H264/90000* - *a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=rtcp-fb:* trr-int 5000* - *a=rtcp-fb:* nack* - *a=rtcp-fb:* nack pli* - *a=rtcp-fb:* ccm fir* - *a=rtcp-fb:* ccm tmmbr* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line	
Reason-Phrase	Not checked
Require	
option-tag	*precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=*(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *packetization-mode=0;profile-level-id=(att-field); * Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted.

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:352* Time description: *-t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF 101* - *b=AS: 315* - *b=RS: 0* - *b=RR: 2500* Attributes for media: - *a=rtpmap: 101 H264/90000* - *a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=rtcp-fb:* trr-int 5000* - *a=rtcp-fb:* nack* - *a=rtcp-fb:* nack pli* - *a=rtcp-fb:* ccm fir* - *a=rtcp-fb:* ccm tmmbr* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition*
Content-Type media-type	*application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 3] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *packetization-mode=0;profile-level-id=(att-field); * Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be "/1" or omitted. Note 3: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

C.26a Generic test procedure for MTSI MT video call - WLAN access to EPC

Test procedure

1) SS sends an INVITE request to the UE.

2) SS may receive 100 Trying from the UE.

3) SS may receive 180 Ringing from the UE.

2A) SS may receive 183 Session Progress from the UE.

2B) SS may send PRACK to the UE to acknowledge the 183 Session Progress.

2C) SS may receive 200 OK for PRACK from the UE.

4) SS may send PRACK to the UE to acknowledge the 180 Ringing Progress.

5) SS may receive 200 OK for PRACK from the UE.

5A) The UE accepts the session invite.

6) SS expects and receives 200 OK for INVITE from the UE, with optionally proper SDP as answer.

7) SS sends ACK to the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
2A	→		183 Session Progress	(Optional) The UE sends 183 response reliably with the SDP answer to the offer in INVITE
2B	←		PRACK	(Optional) SS acknowledges the receipt of 183 response from the UE.
2C	→		200 OK	(Optional) The UE responds to PRACK with 200 OK
3	→		180 Ringing	(Optional) The UE responds to the offer in INVITE with 180 Ringing with the optional SDP answer if SDP answer was not included with 183 Session Progress in step 2A
4	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
5	→		200 OK	(Optional) The UE responds to PRACK with 200 OK.
				SS waits 5 seconds for UE to send 183 Session Progress and/or 180 Ringing or none of the two before proceeding
5A				Make UE accept the video offer.
6	→		200 OK	The UE responds to INVITE with 200 OK and includes SDP answer to acknowledge its current precondition status if SDP answer was not included with 183 Session Progress in step 2A or 180 Ringing in Step 3.
7	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.

NOTE 1: Steps 3, 4, and 5 can happen in parallel to steps 2B and 2C

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:352* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 98 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap: 98 telephone-event/16000* - *a=fmtp: 98 0-15* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF 101* - *b=AS: 315* - *b=RS: 0* - *b=RR: 2500* Attributes for media: - *a=rtpmap: 101 H264/90000* - *a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=rtcp-fb:* trr-int 5000* - *a=rtcp-fb:* nack* - *a=rtcp-fb:* nack pli* - *a=rtcp-fb:* ccm fir* - *a=rtcp-fb:* ccm tmmbr* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 2A)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *Precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *packetization-mode=0;profile-level-id=(att-field); * Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted.

180 Ringing (step 3)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition*
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	length of message-body
Message-body	Optionally present only if there has been no 183 Session Progress with SDP answer at step 2A. Contents if present: Same as specified in step 2A.

200 OK (step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require	Same contents as specified in step 3.
Message-body	Present if there has been no SDP answer at step 2A or step 3. Contents if present: Same as specified in step 2A.

C.26b Generic test procedure for Terminating MTSI Video Call - Fixed Broadband Access to EPC

The generic test procedure for setting up MTSI MT video call over Fixed Broadband access may be performed after successful IMS registration.

Test procedure

1) SS sends an INVITE request to the UE.
2) SS may receive 100 Trying from the UE.
3) SS expects and receives 180 Ringing from the UE.
4) SS sends PRACK to the UE to acknowledge the 180 Ringing
5) SS expects and receives 200 OK for PRACK from the UE.
6) The UE accepts the session invite.
7) SS expects and receives 200 OK for INVITE from the UE.
8) SS sends ACK to the UE.
9) SS sends BYE to the UE.
10) SS expects and receives 200 OK for BYE from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
3	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.(Optional) to have SDP added. If added 180 response is reliably send
4	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
5	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
6				Make the UE accept the video offer.
7	→		200 OK	The UE responds to INVITE with a 200 OK final response after the user answers the call. (Optional) to have SDP added. If not included in 180 response
8	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
9	←		BYE	The SS sends BYE to release the call.
10	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition “IMS security” or “early IMS security” and the condition “SIP Digest without TLS for Fixed Broadband Access” when applicable.

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:352* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99 100* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Media description: *- m=video (transport port) RTP/AVPF 101* *- b=AS: 315* *- b=RS: 0* *- b=RR: 2500* Attributes for media: *- a=rtpmap:1019 H264/90000* *- a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* *- a=rtcp-fb:* trr-int 5000* *- a=rtcp-fb:* nack* *- a=rtcp-fb:* nack pli* *- a=rtcp-fb:* ccm fir* *- a=rtcp-fb:* ccm tmmbr*

180 Ringing (Step 3)

Use the default message "180 Session Progress" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	 *application/sdp*
Message-body	The following SDP types and values shall be present. [Note 3] Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2] Media description: - *m=video (transport port) RTP/AVPF* (fmt) [Note 2] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* [Note 2] - *a=fmtp:* (format) *packetization-mode=0;profile-level-id=(att-field); * Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked Note 3: Parameters for the AMR codec are not checked

200 OK (Step 7)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Message-body	Present if SDP answer was not included with 180 Ringing (Step 3) Contents if present: Same as specified in step 3.

C.27 Generic test procedure for forked response of MTSI MO speech call - EPS

Test procedure:

1) SS responds to the INVITE request with a 183 Session Progress response.

NOTE: Steps 1 to 4 in annex C.21 are performed before this generic test procedure is initiated. This procedure may be performed in parallel with step 5 and later steps in annex C.21.

2) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

3) SS responds to the PRACK request with a 200 OK.

4) SS waits for the UE to send a UPDATE request containing the final SDP offer.

5) SS responds to the UPDATE request with a 200 OK.

6) SS responds to the INVITE request with a 180 Ringing.

7) SS waits for the UE to send a PRACK request.

8) SS responds to the PRACK request with a 200 OK.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	←		183 Session Progress	SS sends an SDP answer.
2	→		PRACK	UE acknowledges and optionally offer a second SDP if a dedicated EPS bearer is established by the network.
3	←		200 OK	SS sends a 200 OK and answers the second SDP if present.
4	→		UPDATE	Optional step: UE sends a second SDP if a dedicated EPS bearer is established by the network.
5	←		200 OK	Optional step: SS sends a 200 OK.
6	←		180 Ringing	SS sends a 180 Ringing.
7	→		PRACK	UE acknowledges.
8	←		200 OK	SS responds PRACK with 200 OK.

Specific Message Contents

183 Session Progress (Step 1)

Use the "183 Session Progress (Step 4)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	different value from common to-tag (invite)

PRACK (Step 2)

Use the "PRACK (Step 5)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note1] Note 1: "o=" line identical to previous SDP sent by UE in the same dialog, except that sess-version is incremented by one if the SDP is not identical to the previous SDP sent by the UE

200 OK for PRACK (Step 3)

Use the "200 OK for PRACK (Step 6)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

UPDATE (Step 4)

Use the "UPDATE (Step 7)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

200 OK for UPDATE (Step 5)

Use the "200 OK for UPDATE (Step 8)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

180 Ringing (Step 6)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

PRACK (Step 7)

Use the default message "PRACK" in annex A.2.4 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

200 OK for PRACK (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

C.28 Generic test procedure for SIP UPDATE after aSRVCC/bSRVCC handover failure/cancelled - EPS

Test procedure:

1) SS waits for the UE to send an UPDATE request containing a final SDP offer.

2) SS responds to the UPDATE request with a 200 OK.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		UPDATE	UE sends UPDATE.
2	←		200 OK	SS sends a 200 OK.

Specific Message Contents

UPDATE (Step 1)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Reason	
protocol	*SIP*
reason-params	*cause=487; text="handover cancelled"*, if this procedure is performed after aSRVCC/bSRVCC handover cancelled. Text would be present if release >= 10 and rel-9 can omit the text *cause=487; text="failure to transition to CS domain"*, if this procedure is performed after aSRVCC/bSRVCC handover failure. Text would be present if release >= 10 and rel-9 can omit the text
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] [Note 4] - *a=fmtp:*(format) [Note 2, 3] - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv or* *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked. Note 3: Parameters for the AMR codec are not checked. Note 4: The AMR channel number shall be "/1" or omitted.

200 OK for UPDATE (Step 2)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Content-Length	
Value	length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media.

C.29 Generic test procedures for Supplementary Services - EPS

C.29.1 Procedures for activation and deactivation of Supplementary Services - EPS

Generic test procedure for signalling between UE and XCAP server to activate or deactivate a supplementary service.

Test procedure:

0a) Pre-configurations:

In case of EUTRA

- The UE is IMS registered before any activation or deactivation of Supplementary Services is triggered. This will ensure more deterministic UE behaviours.
- The UE has established a 2nd PDN connectivity for IMS XCAP signalling. In case of EUTRA the UE may either be configured to re-use the Internet APN for XCAP signalling or the UE uses a specific XCAP-only APN:
  - in case of Internet APN the PDN connectivity is established during the initial registration procedure according to TS 36.508 clause 4.5.2 [94] applying XCAP_SIGNALLING.
  - in case of a specific XCAP-only APN the generic procedure according to TS 36.508 clause 4.5A.14 [94] shall be applied.
- During these procedures the UE may request a DNS server address via NAS signalling and as parallel behaviour the UE may resolve the IP address of the XCAP server via DNS.

In case of WLAN the UE is configured to use XCAP requests with PDN according TS 36.508 clause 4.5A.25 or without any PDN connection according A.12/49 3GPP TS 34.229-2 [5].

In case of fixed broadband access, the UE is configured to use XCAP requests according A.12/50 TS 34.229-2 [5].

0b) At the SS an HTTP server is established at port 80 to simulate the XCAP server.

NOTE: TLS is not a test requirement i.e. the UE uses port 80 to access XCAP and BSF servers and SS does not redirect the UE to use HTTPS (port 443).

1) Activation of the specific Supplementary Service is triggered at the UE with appropriate MMI command.

2) The UE sends an initial HTTP request to the SS.

3) In case of HTTP Digest XCAP authentication when the UE does not provide correct authorization credentials within its initial request:

3a) the SS shall challenge the UE by sending a “401 Unauthorized” response to it.
When the UE supports GBA for XCAP authentication and GBA shall be used according to test requirements or test configuration, the SS shall indicate bootstrapped security association is required as specified in TS 24.109 [119] clause 5.2.4 and the generic procedure according to C.29.2 shall be applied.

3b) the UE repeats the HTTP request including a valid digest response in the authorization header.
The SS shall check the digest response taking into account the user’s prearranged password for (pure) HTTP digest authentication, or, for GBA, being derived from the key material (Ks) using key derivation function as specified in 3GPP TS 33.220 [120].

4) The SS sends a 200 (OK) response

5) Optionally UE and SS exchange a sequence of additional HTTP requests and responses. In this sequence the UE may query the contents of the simservs document or selected parts of it.

In general the HTTP requests are responded with a 200 “Ok” response but in case of a GET request to a non-existing node the SS shall respond with a 404 “File Not Found”.

6) The simservs document is checked according to specific test requirements.

7) Deactivation of supplementary service is triggered at the UE with appropriate MMI command.

8) UE and SS exchange a sequence of HTTP requests and responses. In this sequence the UE may query the contents of the simservs document or selected parts of it.
In general the HTTP requests are responded with a 200 “Ok” response but in case of a GET request to a non-existing node the SS shall respond with a 404 “File Not Found”.

9) The simservs document is checked according to specific test requirements.

Expected sequence:

Step	Direction UE	Direction SS	Message/Procedure	Comment
1			Make the UE attempt activation of supplementary service	
2	→		Initial HTTP Request	NOTE 1
3			EXCEPTION: steps 3a and 3b describe behaviour in case of HTTP Digest XCAP authentication when the UE does not provide correct authorization credentials within its initial request	
3a	←		HTTP Response: “401 Unauthorized”	
			EXCEPTION: By default, when the UE supports GBA for XCAP authentication, GBA shall be used according to the generic test procedure C.29.2. NOTE: See TS 34.229-2 [5] for cases where the default does not apply.	(optional) GBA authentication at BSF server
3b	→		HTTP Request with valid authorization credentials	The SS checks the digest response
4	←		HTTP Response: “200 OK”	
5			EXCEPTION: steps 5a and 5b describe further optional message exchange between the UE and the SS; steps 5a and steps 5b can be repeated several times this exchange of information is considered to be finished when there is no further HTTP request sent by the UE within 20 seconds after the previous request	
5a	→		HTTP Request	NOTE 1
5b	←		HTTP Response: “200 OK” or “404 File Not Found”	NOTE 3
6			Check: Does the simservs document stored in the SS contain the information supplied by the UE as required by the test requirements of the specific test case?	This is done by fetching the whole simservs document from the XCAP server and checking its content against the respective XML file (according to the XSD definitions for the respective supplementary service)
7			Make the UE attempt deactivation of supplementary service	
8			EXCEPTION: steps 8a and 8b describe the mandatory message exchange between the UE and the SS which can be repeated several times; this exchange of information is considered to be finished when there is no further HTTP request sent by the UE within 10 seconds after the previous request	
8a	→		HTTP Request	NOTE 1
8b	←		HTTP Response: “200 OK” or “404 File Not Found”	NOTE 3
9			Check: Does the simservs document stored in the SS contain the information supplied by the UE as required by the test requirements of the specific test case?	This is done by fetching the whole simservs document from the XCAP server and checking its content against the respective XML file (according to the XSD definitions for the respective supplementary service)
NOTE 1: The HTTP requests sent by the UE are processed by an XCAP server implementation at the SS to modify the contents of the simservs document. NOTE 2: Void. NOTE 3: “404 File Not Found” is sent as response for a GET request to a non-existing node				

Specific Message Contents

HTTP Requests sent by the UE (step 2, 3b, 5a, 8a)

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 2616 [69]
Method		*GET, PUT, DELETE*		
Request-URI		XCAP URI referring to the simservs document as specified in RFC 4825 [70]; the document selector of such XCAP URI consists of - Configured XCAP root URI - *simservs.ngn.etsi.org* - *users* - same public user id as the default public user identity received in P-Associated-URI header in 200 OK for REGISTER (NOTE 4). - *simservs.xml* (in this order, separated by a slash); According to RFC 4825 [70] the node selector of the XCAP URI shall identify a valid part of a simservs document or whole document itself (NOTE 2).		
Version		*HTTP 1.1*		
User-Agent	A1			RFC 2616 [69]
Product token		*3gpp-gba*		TS 24.109 [119]
Authorization		present in case of HTTP Digest XCAP authentication in the initial request or in the request following the "401 Unauthorized" response *Digest*		RFC 2617 [16] RFC 3310 [17]
username	NOT A2	As configured in the UE (NOTE 5). Same public user id as the default public user identity received in P-Associated-URI header in 200 OK for REGISTER (NOTE 6).		
username	A2	B-TID as obtained from GBA authentication		
realm		same value as received in the realm directive in the WWW Authenticate header sent by SS		
nonce		same value as in WWW-Authenticate header sent by SS		
opaque		same value as sent by the SS in "401 Unauthorized"		
digest-uri		same URI as used in Request-URI		
qop-value		*auth*		
cnonce-value		value assigned by UE affecting the response calculation		
nonce-count		1		
response	NOT A2	response calculated by UE using prearranged password		
response	A2	response calculated by UE using password derived from the key material of the GBA authentication according to Generic key derivation as specified in Annex B.3 of TS 33.220 [120] using static string "gba-me" as parameter P0 in Annex B.3.		
algorithm		*MD5*		
Content-Type		present for HTTP PUT method		RFC 2616 [69]
media-type		*application/vnd.etsi.simservs+xml* or *application/xcap-el+xml* or *application/xcap-att+xml* (NOTE 3)		
Message-body		present for HTTP PUT method: XML fragment of given node		RFC 2616 [69] RFC 4825 [70]

NOTE 1: Any other headers are ignored.
NOTE 2: The SS shall check and make sure that the syntax of the node selector expressions is in compliance to clause 6.2 of RFC 4825 [70].
NOTE 3: the media-type depends on the kind of node being accessed by the Request-URI: document, element or attribute (see RFC 4825 [70]).
NOTE 4: According A.12/38 3GPP TS 34.229-2 [5].
NOTE 5: Shall be present if A.12/37 3GPP TS 34.229-2 [5] is yes.
NOTE 6: Shall be present if A.12/37 3GPP TS 34.229-2 [5] is no.

Condition	Explanation
A1	UE supports GBA authentication

A2	GBA authentication shall be applied (according to test requirements or test configuration)

HTTP Responses (step 4, 5b, 8b2) – normal case

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 2616 [69]
Version		*HTTP 1.1*		
Code		*200*		
Reason		*OK*		
Server				RFC 2616 [69]
product		*XCAP-Server*		
Date				RFC 2616 [69]
HTTP-date		valid date according to RFC 2616 [69] section 3.3.1		
ETag				RFC 2616 [69]
entity-tag		hextring: value starting with "478fb2358f700" and incremented after each PUT operation		
Content-Type media-type		present for HTTP GET method *application/vnd.etsi.simservs+xml* or *application/xcap-el+xml* or *application/xcap-att+xml* (NOTE 1)		RFC 2616 [69]
Content-Length				RFC 2616 [69]
value		length of the message body		
Message-body		present for GET method: XML fragment of given node		RFC 2616 [69] RFC 4825 [70]
NOTE 1: the media-type depends on the kind of node being accessed with the HTTP GET method: document, element or attribute (see RFC 4825 [70]).				

HTTP Responses (step 5b, 8b) – Response for GET request to a non-existing node

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 2616 [69]
Version		*HTTP 1.1*		
Code		*404*		
Reason		*File Not Found*		
Server				RFC 2616 [69]
product		*XCAP-Server*		
Date				RFC 2616 [69]
HTTP-date		valid date according to RFC 2616 [69] section 3.3.1		

HTTP Response (step 3a) for HTTP Digest XCAP authentication

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 2616 [69]
Version		*HTTP 1.1*		
Code		*401*		
Reason		*Unauthorized*		
Server				RFC 2616 [69]
product		*XCAP-Server*		
Date				RFC 2616 [69]
HTTP-date		valid date according to RFC 2616 [69] section 3.3.1		
WWW-Authenticate				RFC 2616 [69]
realm	NOT A1	home domain name as stored in EF_{DOMAIN} or home domain name derived from the IMSI		
realm	A1	containing two parts delimited by "@" (see TS 24.109 [119] clause 5): - *3GPP-bootstrapping* - home domain name as stored in EF_{DOMAIN} or home domain name derived from the IMSI		
algorithm		*MD5*		
qop-value		*auth*		
nonce		Base 64 encoding of RAND and AUTN		
opaque		arbitrary value (to be returned by the UE in subsequent request)		

Condition	Explanation
A1	UE supports GBA authentication and GBA authentication shall be applied (according to test requirements or test configuration)

C.29.2 Procedure for GAA XCAP authentication

The generic test procedure for GBA authentication between UE and BSF.

The generic test procedure for GAA XCAP authentication is referred to the bootstrapping procedure in TS 33.220 [120], clause 4.5.2 and TS 24.109 [119] clause 4.2.

Test procedure:

0a) Pre-configurations:
The UE may resolve the IP address for the BSF server via DNS.

0b) At the SS an HTTP server is established at port 80 to simulate the BSF server.

1) UE sends initial GET to the BSF server.

2) BSF server responds with “401 Unauthorized”.

3) UE sends GET with Authorization header to the BSF server.

4) BSF server responds with "200 OK" when the UE has provided a valid Authorization header.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		HTTP Request	
2	←		HTTP Response: “401 Unauthorized”	
3	→		HTTP Request with valid authorization credentials	
4	←		HTTP Response: “200 OK”	

Specific Message Contents

HTTP Request (step 1)

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI Version		 *GET* Request-URI *HTTP/* DIGIT.DIGIT		RFC 2616 [69]
Host host		 *bsf.*mnc<MNC>.mcc<MCC>*.pub.3gppnetwork.org* (when no ISIM available on the UICC) , optionally followed by port 80 or *bsf.*domain name (when using ISIM) , optionally followed by port 80		RFC 2616 [69]
User-Agent Product token		 *3gpp-gba-tmpi*		RFC 2616 [69] TS 24.109 [119]
Authorization username realm nonce digest-uri response		*Digest* private user identity as stored in EF_{IMPI} (when using ISIM) or private user identity derived from IMSI (when no ISIM available on the UICC) or the value of the TMPI if one has been associated with the private user identity as described in 3GPP TS 33.220 [120] *bsf.*mnc<MNC>.mcc<MCC>*.pub.3gppnetwork.org* (when no ISIM available on the UICC) or *bsf.*domain name (when using ISIM) empty value absoluteURL http://<BSF address>/ or abs_path "/" empty value		RFC 2616 [69] RFC 2617 [16] RFC 3310 [17]

NOTE 1: All choices for applicable conditions are described for each header.

HTTP Response (step 2)

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 2616 [69]
Version		*HTTP/1.1*		
Code		*401*		
Reason		*Unauthorized*		
Server				RFC 2616 [69]
product		*BSF-Server*		
Date				RFC 2616 [69]
HTTP-date		valid date according to RFC 2616 [69] section 3.3.1		
WWW-Authenticate				RFC 2616 [69]
challenge		*Digest*		RFC 2617 [16]
realm		same value as received in step 1		
algorithm		*AKAv1-MD5*		
qop-value		*auth-int*		
nonce		Base 64 encoding of RAND and AUTN		
opaque		*5ccc069c403ebaf9f0171e9517f30e41*		

HTTP Request (step 3)

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 2616 [69]
Method		*GET*		
Request-URI		Request-URI		
Version		*HTTP/* DIGIT.DIGIT		
Host				RFC 2616 [69]
host		*bsf.*mnc<MNC>.mcc<MCC>*.pub.3gppnetwork.org* (when no ISIM available on the UICC), optionally followed by port 80 or *bsf.*domain name (when using ISIM), optionally followed by port 80		
Authorization		*Digest*		RFC 2616 [69] RFC 2617 [16]
username		private user identity as stored in EF_{IMPI} (when using ISIM) or private user identity derived from IMSI (when no ISIM available on the UICC) or the value of the TMPI if one has been associated with the private user identity as described in 3GPP TS 33.220 [120]		RFC 3310 [17]
realm		same value as received in the realm directive in the WWW Authenticate header sent by SS		
opaque		*5ccc069c403ebaf9f0171e9517f30e41*		
digest-uri		absoluteURL http://<BSF address>/ or abs_path "/"		
cnonce-value		value assigned by UE affecting the response calculation		
nonce-count		*00000001*		
response		response calculated by UE		
algorithm		*AKAv1-MD5*		

NOTE 1: All choices for applicable conditions are described for each header.

HTTP Response (step 4)

Header/param	Cond	Value/remark	Rel	Reference
Status-Line Version Code Reason		 *HTTP/1.1* *200* *OK*		RFC 2616 [69]
Server Product token		 *3gpp-gba-tmpi*		RFC 2616 [69]
Date HTTP-date		 valid date according to RFC 2616 [69] section 3.3.1		RFC 2616 [69]
Authentication-Info message-qop rspauth cnonce nc		 *qop=auth-int* see Note 1 same value as received in step 3 *1*		RFC 2616 [69] RFC 2617 [16]
Content-Type media-type		 *application/vnd.3gpp.bsf+xml*		RFC 2616 [69]
Content-Length value		 length of the message body		RFC 2616 [69]
Message-body		*<?xml version="1.0" encoding="UTF-8"?>* *<BootstrappingInfo xmlns="uri:3gpp-gba">* *<btid>*B-TID*</btid>* *<lifetime>*key lifetime*</lifetime>* *</BootstrappingInfo>* with - B-TID Bootstrapping - Transaction Identifier according to TS 33.220 [120] clause 4.5.2: base64encode(RAND)@BSF_servers_domain_name - key lifetime lifetime of the key material formatted according to XSD dateTime data type		RFC 2616 [69] TS 24.109 Annex C [119]

NOTE 1: Rspauth is computed according to RFC 3310 and RFC 2617.

C.30 Generic test procedure for Mobile Initiated Deregistration - EPS

The generic test procedure:

IMS deregistration is initiated on the UE. SS waits for the UE sending a REGISTER request, in accordance with 3GPP TS 24.229 [10], clause 5.1.1.6.

Expected sequence:

Step	Direction		Message/Procedure	Comment
	UE	SS		
0A	→		SUBSCRIBE	Optional: The UE unsubscribes from one of its subscribed to event packages
0B	←		200 OK	If the UE sent SUBSCRIBE, the SS responds to SUBSCRIBE with 200 OK
0C	←		NOTIFY	If the UE sent SUBSCRIBE, the SS sends a final NOTIFY
0D	→		200 OK	Optional: If the UE sent SUBSCRIBE, the UE responds to NOTIFY with 200 OK
1	→		REGISTER	The UE sends deregistration for IMS services
2	←		200 OK	The SS responds to REGISTER with 200 OK
Note 1: Steps 0A-0D may be repeated for any or all event packages subscribed to by the UE. It is the UE's decision which unsubscriptions to perform. Note 2: The UE can send the 200 OK for NOTIFY after the REGISTER request or even not send it at all.				

Specific message contents

SUBSCRIBE (step 0A)

Use the default message "SUBSCRIBE for reg-event package" in annex A.1.4 or "SUBSCRIBE for conference event package" in annex A.5.1 or "SUBSCRIBE for message-summary event package" in annex A.6.1 with the following exceptions:

Header/param	Value/remark
From addr-spec tag	 Same as in original SUBSCRIBE that set up the corresponding subscription Same as in original SUBSCRIBE that set up the corresponding subscription
To addr-spec tag	 As specified in A.1.4/A.5.1/A.6.1 Same as in 200 OK for original SUBSCRIBE that set up the corresponding subscription
CSeq value method	 value of the previous SUBSCRIBE sent by the UE for this dialog incremented by one *SUBSCRIBE*
Session-ID sess-id	 Same as in original SUBSCRIBE that set up the corresponding subscription (if present in original SUBSCRIBE)
Expires delta-seconds	 *0*

200 OK for SUBSCRIBE (step 0B)

Use the default message "200 OK for SUBSCRIBE" in annex A.1.5, A.5.2 or A.6.3 whatever appropriate, with the following exceptions:

Header/param	Value/remark
To addr-spec tag	 As specified in A.1.4/A5.1/A.6.1 Same as in step 0A
Expires delta-seconds	 *0*

NOTIFY (step 0C)

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *NOTIFY* UE's contact address in SIP URI form, as provided in the Contact header within the SUBSCRIBE creating the dialog *SIP/2.0*		RFC 3261 [15]
Via **via-parm1:** Sent-protocol sent-by sent-by via-branch **via-parm2:** sent-protocol sent-by via-branch	 A1 A2, A6	order of the parameters in this header must be like in this table *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP IP address and protected server port of SS IP address and unprotected server port of SS (optional) value starting with '*z9hG4bK'* (NOTE 1) *SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP *scscf.3gpp.org* value starting with '*z9hG4bK'* (NOTE 1)		RFC 3261 [15]
From addr-spec tag		 same URI as received in the To header of the corresponding SUBSCRIBE message same as to-tag in step 0A		RFC 3261 [15]
To addr-spec tag		 same URI as received in the From header of the corresponding SUBSCRIBE message same as from-tag in step 0A		RFC 3261 [15]
Call-ID callid		 same as value received in SUBSCRIBE message		RFC 3261 [15]
CSeq value method	A1,A2	 1 *NOTIFY*		RFC 3261 [15]
Contact addr-spec	 A3	 *<sip:scscf.3gpp.org>*		RFC 3261 [15]
addr-spec	A4	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName		
addr-spec	A5	*<scscf.3gpp.org>*		
Event event-type	 A3	 *reg*		RFC 6665 [140] RFC 3680 [22]
event-type	A4	*conference*		
event-type	A5	*message-summary*		
Max-Forwards value		 *69*		RFC 3261 [15]
Subscription-State substate-value		 *terminated*		RFC 6665 [140]
Content-Length value		 *0*		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5]
A3	Final NOTIFY sent for reg-event
A4	Final NOTIFY sent for conf-event
A5	Final NOTIFY sent for message-summary
A6	SIP Digest without TLS for Fixed Broadband Access (SIP Digest without TLS, A.6a/5 3GPP TS 34.229-2 [5])

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

200 OK (step 0D)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE"

REGISTER (step 1)

Use the default message “REGISTER” in annex A.1.1 with conditions A2 (IMS Security) or A3 (GIBA), as applicable, in accordance to 3GPP TS 24.229 [10] clause 5.1.1.6, and A17 "UE initiated IMS re-registration or de-registration" with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and protected server port of the UE in case of IMS security (A2 of A.1.1) or unprotected port of the UE (optional) in case of GIBA (A3 of A.1.1) and, if the UE supports GRUU, the following parameter: +*sip.instance*="<*urn:gsma:imei:* (gsma-specifier-defined-substring)>” or *
expires	*0* (if present)
Expires	(must be present if addr-spec is *)
delta-seconds	*0* (if present)
Supported	header may be missing or it may contain any value
Authorization	value not checked

NOTE: In contrast to A.1.1, the Contact header does not have any further mandatory feature parameters.

200 OK (step 2)

Use the default message “200 OK for REGISTER” in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	same value as in REGISTER request if "*" is not included in the Contact header field of the REGISTER request in step 1 same value as in the Contact header field of the "200 OK" response to the initial registration if "*" is included in the Contact header field of the REGISTER request in step 1 (NOTE)
expires	0
NOTE: According to 3GPP TS 24.229 [10] clause 5.4.1.4.1 when the S-CSCF gets a wild-carded contact address for de-registration it shall include all de-registered contact addresses in the contact header of the 200 OK response ⇒ there is no “*” in DL.	

C.30a Void

C.30b Generic test procedure for UE Initiated Deregistration - Fixed Broadband Access to EPC

The generic test procedure:

IMS deregistration is initiated on the UE. SS waits for the UE sending a REGISTER request, in accordance with 3GPP TS 24.229 [10], clause 5.1.1.6.

Expected sequence:

Same as described in Annex C.30

Specific message contents

The default messages contents in Annex C.30 are used with condition “SIP Digest without TLS for Fixed Broadband Access” when applicable

C.31 Generic test procedure for media re-establishment after unsuccessful SRVCC handover - EPS

Test procedure:

1) UE sends a re-INVITE request to the SS.

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with a 200 OK.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with audio re-established.
2	←		100 Trying	SS sends a 100 Trying provisional response.
3	←		200 OK	SS responds to INVITE with a 200 OK final response.
4	→		ACK	UE acknowledges the receipt of 200 OK for INVITE.

Specific Message Contents

INVITE (Step 1)

Use the default message “INVITE for MO Call” in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark	Rel
Request-Line Method Request-URI SIP-Version	 *INVITE* Same value as the URI from the Contact header of the original INVITE request as sent by SS *SIP/2.0*	
Reason	Reason header field with Protocol "SIP" and reason parameter "cause" with value "487"	
	reason-text set to "handover cancelled" or “failure to transition to CS domain”	Rel-10
Message Body	The following SDP types and values. Session description: - *v=0* - *o=*(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 2] - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=(start-time) (stop-time)* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000/1* - *a=fmtp:*(format) Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE, except that sess-version is incremented by one if the SDP is not identical to the previous SDP sent by the UE	

200 OK (Step 3)

Use the default message “200 OK” in annex A.3.1 with the following exceptions:

Header/param	Value/Remark
Contact addr-spec	 Same value as the URI from the Contact header of the original INVITE request as sent by SS
Content-Type media-type	 application/sdp
Content-Length value	 length of message-body
Message Body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111* (sess-version) *IN* (addrtype) (unicast-address for SS) [Note 3] - - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS*:37 Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1] - *c=IN* (addrtype) (connection-address for SS) [Note 1] - *b=AS:*37 - *b=RS:* (bandwidth-value) [Note 2] - *b=RR:* (bandwidth-value) [Note 2] Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000/1* [Note 1] *a=fmtp:*(format) mode-change-capability=2; max-red=220 [Note 1] Attributes for preconditions: - a=curr:qos local sendrecv a=curr:qos remote sendrecv a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv Note 1: The value for fmt, payload type (AMR) and format is copied from step 1 Note 2: The bandwidth-value is copied from step 1. Note 3: sess-version incremented by one if SDP changed compared to last SDP sent by SS.

ACK (Step 4)

Use the default message "ACK" in annex A.2.7 with condition A5 and the following exceptions:

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 ACK Same value as the URI from the Contact header of the original INVITE request as sent by SS SIP/2.0		RFC 3261 [15]
To addr-spec tag		 Same value as used in the INVITE of step 1 Same value as used in the INIVTE of step 1		RFC 3261 [15]

NOTE 1: when A.2.7 refers to "INVITE", the re-INVITE of step 1 is meant.

C.32 Generic test procedure for MO release of IMS call - EPS

The generic test procedure:

1) SS makes the UE release the IMS call. SS sends AT command CHCCS [123].

2) Call is released on the UE. SS waits the UE to send a BYE request.

3) SS responds to the BYE request with valid 200 OK response.

4)-5) Deactivation of a dedicated EPS Bearer during call establishment.

Steps 4 and 5 are applicable for a UE with E-UTRA support (TS 34.229-2 A.18/1) only.

Expected sequence

Step	Direction		Message/Procedure	Comment
	UE	SS		
1				Make the UE release the IMS call
2	→		BYE	The UE releases the call with BYE
3	←		200 OK	The SS sends 200 OK for BYE
4-5				EPS Bearer Deactivation procedure according TS 36.508 [94] subclause 4.5A.15.

Specific message contents

None.

C.32a Generic test procedure for MO release of IMS emergency call (when IMS emergency registration had failed)

The generic test procedure:

1)-3) MO Call release according to procedure C.32, steps 1-3.

4-5) Void.

6)-7) Wait for optional PDN DISCONNECT REQUEST from UE and deactivation of a default emergency EPS Bearer.

Expected sequence

Step	Direction		Message/Procedure	Comment
	UE	SS		
1-3			Steps 1-3 defined in annex C.32	MO Call release
4-5				Void
6-7				EPS Bearer Deactivation procedure according TS 36.508 [94] subclause 4.5A.15A.

Specific message contents

None.

C.32b Void

C.33 Generic test procedure for MT release of IMS call - EPS

The generic test procedure:

1) SS sends BYE to the UE.

2) SS expects and receives 200 OK for BYE from the UE.

3)-4) Deactivation of a dedicated EPS Bearer during call establishment.

Steps 3 and 4 are applicable for a UE with E-UTRA support (TS 34.229-2 A.18/1) only.

Expected sequence

Step	Direction		Message/Procedure	Comment
	UE	SS		
1	←		BYE	The SS sends BYE to release the call.
2	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.
3-4				EPS Bearer Deactivation procedure according TS 36.508 [94] subclause 4.5A.15.

Specific message contents

C.34 Generic test procedure for removal of early dialog of origination call after successful aSRVCC handover - EPS

Test procedure:

1) SS sends 404 Not found to the UE

2) SS waits for UE to send ACK

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	←		404 Not Found	SS sends 404 Not Found
2	→		ACK	UE sends ACK.

ACK (step 2)

Use the default message " ACK” in annex A.2.7 with condition A4.

C.35 Generic test procedure for removal of early dialog of incoming call after successful aSRVCC handover - EPS

Test procedure:

1) SS sends CANCEL to the UE
2) SS waits for UE to send 200 OK
3) SS waits for UE to send 487 Request terminated
4) SS responds with ACK to the UE

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	←		CANCEL	SS sends CANCEL
2	→		200 OK	UE sends 200 OK.
3	→		487 Request Terminated	UE sends 487 Request Terminated
4	←		ACK	SS sends ACK

ACK (step 2)

Use the default message " ACK" in annex A.2.6 with condition A4.

C.36 Generic test procedure for removal IMS session release after SRVCC CS+PS Handover - EPS

Test procedure:

1) SS sends BYE to UE

2A) SS waits for UE to send 200 OK

2B) SS waits for UE to send 481 Call/Transcation Does Not Exist

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	←		BYE	SS sends BYE
				Exception: Based on the UE implementation, either IMS session is removed internally or will be terminated explicitly. If UE does not delete the IMS session, then, UE sends 200 OK otherwise '481 Call/Transcation Does Not Exist
2A	→		200 OK	UE sends 200 OK.
2B	→		SIP 481 Call/Transaction Does Not Exist	UE sends 481 Call/Transcation Does Not Exist

C.37 Generic test procedure for Inviting user to Video conference by sending a REFER request to the conference focus - EPS

Test procedure

1) UE invites a user to the conference created. SS waits the UE to send to the conference focus a REFER request, which refers to the user to be invited to the conference.

2) SS responds to the REFER request with a valid 202 Accepted response.

3) SS sends an initial NOTIFY to tell that the invited user is trying to join the conference.

4) UE responds to the NOTIFY request with valid 200 OK response.

5) SS sends the final NOTIFY to tell that the invited user has successfully joined the conference.

6) UE responds to the NOTIFY request with a valid 200 OK response.

7) Optional: If UE subscribed the conference event package during the generic test procedure of Annex C.10, SS sends a NOTIFY for the conference event package to the UE to notify that the user joined the conference.

8) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REFER	UE sends REFER to SS referring to the conference
2	←		202 Accepted	The SS responds with a 202 final response
3	←		NOTIFY	The SS sends initial NOTIFY for the implicit subscription created by the REFER request
4	→		200 OK	The UE responds the NOTIFY with 200 OK
5	←		NOTIFY	The SS sends a NOTIFY related to REFER request to confirm that the invited user was able to join the conference
6	→		200 OK	The UE responds the NOTIFY with 200 OK
7	←		NOTIFY	Optional: If the UE has subscribed the conference event package, the SS sends a NOTIFY for conference event package to inform that the invited user was able to join the conference
8	→		200 OK	Optional: The UE responds the NOTIFY with 200 OK

Specific Message Contents

REFER (Step 1)

Use the default message “MO REFER” in annex A.2.10 with the following exceptions:

Header/param	Value/remark
Request-URI	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
Refer-To	
addr-spec	SIP URI or tel URI of the user invited to the conference. If an active session exists, the Replaces header in the header portion of the SIP URI shall be included (mandatory inclusion is stated in IR.92 [133]) and set to the dialog ID of the active session according to RFC 3891. In this case, if the user has been invited with a tel URI, the UE shall convert the tel URI to a SIP URI according to RFC 3261 [15] clause 19.1.6. (NOTE: the dialog ID is percent encoded according to RFC 3986).
To	
addr-spec	*sip:final@conf-factory.* appended with px_IMS_HomeDomainName
tag	remote tag of the dialog with the conference focus created in step 2 of C.10
Route	
route-param	URIs of the Record-Route header of 183 response sent in step 4 of C.38 in reverse order

NOTIFY (Step 3)

Use the default message “MT NOTIFY for refer package” in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

NOTIFY (Step 5)

Use the default message “MT NOTIFY for refer package” in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

NOTIFY (Step 7)

Use the default message “NOTIFY for conference event package” in annex A.5.3 with the following exceptions:

Header/param	Value/remark
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<conference-info xmlns="urn:ietf:params:xml:ns:conference-info">* *entity="sip:final@conf-factory.* appended with px_IMS_HomeDomainName*"* *state="partial"* *version="1"* *<users>* *<user entity="* **SIP URI or tel URI of the invited user***">* *<endpoint entity="* **Contact URI of the invited user***">* *<status>connected</status>* *<joining-method>dialed-in</joining-method>* *<media id="1">* *<type>audio</type>* *<label>11223</label>* *<src-id>***random SSRC value***</src-id>* *<status>sendrecv</status>* *</media>* *<media id="2">* *<type>video</type>* *<label>11224</label>* *<src-id>***random SSRC value***</src-id>* *<status>sendrecv</status>* *</media>* *</endpoint>* *</users>* *</conference-info>*

C.38 Generic test procedure for MTSI Video conference creation - EPS

Test procedure

1-8) UE creates the video conference. The same message sequence as in steps 1 - 8 of Annex C.25 are used to create the conference into the conference focus and negotiate the media.

9) SS responds to the INVITE request with valid 200 OK response.

10) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

11) SS waits the UE to optionally subscribe to the conference event package with a SUBSCRIBE message

12) If UE sent SUBSCRIBE, SS responds to it with 200 OK response.

13) If UE sent SUBSCRIBE, SS sends a NOTIFY for the conference event package to the UE.

14) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS video conference call	
2-8			Steps 2-8 of Annex C.25	The same messages as in steps 2 - 8 of Annex C.25
9	←		200 OK	The SS responds INVITE with 200 OK and gives the final conference URI within the response
10	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
			EXCEPTION: steps 11 – 14 describe optional behaviour depending on UE configuration. The SS shall wait up to 3s for the SUBSCRIBE of step 10	
11	→		SUBSCRIBE	UE subscribes the conference event
12	←		200 OK	SS responds to the subscription
13	←		NOTIFY	SS sends the initial state of the conference event to the UE
14	→		200 OK	UE responds to the NOTIFY

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable

Specific Message Contents

The specific message contents for steps 1 – 8 is otherwise identical to what have been specified in Annex C.25, but with the exceptions to steps 1 and 3 as below:

INVITE (Step 2)

Header/param	Value/remark
Request-Line	
Request-URI	*sip:mmtel@conf-factory* appended with px_IMS_HomeDomainName
To	
addr-spec	*sip:mmtel@conf-factory* appended with px_IMS_HomeDomainName

183 Session in Progress for INVITE (Step 4)

Header/param	Value/remark
Contact	
addr-spec	*sip:temporary@conf-factory.* appended with px_IMS_HomeDomainName
feature-param	*isfocus*
Record-Route	
rec-route	*<sip:orig@scscf.3gpp.org;lr>,* *<sip:SS P-CSCF address: protected server port of SS;lr>*

200 OK for INVITE (Step 9)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Record-Route	
rec-route	Same value as in the 183 response
Contact	
addr-spec	*sip:final@conf-factory*. appended with px_IMS_HomeDomainName
feature-param	*Isfocus*

ACK (Step 9)

Use the default message "ACK" in annex A.2.7 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	*sip:final@conf-factory*. appended with px_IMS_HomeDomainName

SUBSCRIBE (Step 10)

Use the default message "SUBSCRIBE for conference event package" in annex A.5.1

200 OK (Step 11)

Use the default message "200 OK for SUBSCRIBE" in annex A.5.2.

C.38a Generic test procedure for MTSI Video conference creation - WLAN access to EPC

Test procedure

1-3) UE creates the video conference. The same message sequence as in steps 1 - 3 of Annex C.25a are used to create the conference into the conference focus and negotiate the media.

4-9) SS and UE complete the creation of the video conference. The same message sequence as in step 9-14 of Annex C.38 is used to complete the video conference.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS video conference call	
2-3			Steps 2-3 of Annex C.25a	The same messages as in steps 2 - 8 of Annex C.25a
4-9			Step 9-14 of Annex C.38	The same messages as in steps 9 - 14 of Annex C.38

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable.

Specific Message Contents

The specific message contents for steps 2-3 is otherwise identical to what have been specified in Annex C.25a and for steps 4-9 is otherwise identical to what have been specified in Annex C.38, but with the exceptions as below:

200 OK for INVITE (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Record-Route rec-route	 Same value as in the 180 response
Contact addr-spec feature-param	 *sip:final@conf-factory*. appended with px_IMS_HomeDomainName *Isfocus*
Require option-tag	 *precondition*
Message-body	same SDP types and values as for C.21a Step 4 (180 Ringing)

C.39 Generic test procedure for setting up MTSI MO speech call for rSRVCC - EPS

Test procedure:

1) MO speech is initiated on the UE as a result of receiving information from the lower layers that the CS to PS SRVCC access transfer is initiated. The call is initiated towards the URI of the STI-rSR as received during registration.
2) UE sends an INVITE request to the SS.
3) SS responds to the INVITE request with a 100 Trying response.
4) SS responds to the INVITE request with a 200 OK.
5) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			UE attempt an IMS speech call a result of an initiation of the rSRVCC procedure	
2	→		INVITE	UE sends INVITE with the first SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		200 OK	SS responds INVITE with 200 OK.
5	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Request-Line	
Request-URI	sip:sti-sr@atcf.visited2.net NOTE: This value was received by the UE in the preceeding registration procedure
To	
addr-spec	sip:sti-sr@atcf.visited2.net NOTE: This value was received by the UE in the preceeding registration procedure
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=-(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - b=AS: (bandwidth-value) - *b=RS*: (bandwidth-value) [Note 7] - *b=RR*: (bandwidth-value) [Note 7] Attributes for media: - *a=rtpmap*: (payload type) *AMR-WB/16000* [Note 8] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 9] - *a=rtpmap*: (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=ecn-capable-rtp: leap ect=0* [Note 3] - *a=rtcp-fb:* nack ecn* [Note 3] - *a=rtcp-xr:ecn-sum* [Note 3] - *a=rtcp-rsize* [Note 3] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 4] - *a=a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20|1:4FEC_ORDER=FEC_SRTP"* [Note 4] Note 1: At least one "c=" field shall be present. Note 2: Void. Note 3: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 4: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 5: Void Note 6: Void Note 7: The RR value must be greater than 0. The RS value can be any value. Note 8: The AMR channel number shall be "/1" or omitted. Note 9: values from 0 to 220 are allowed

200 OK for INVITE (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/Remark
Content-Type	
media-type	*application/sdp*
Feature-Caps	
feature-param	*+g.3gpp.ti=* (value) Note: The value of this parameter shall be the same as the Transaction Identifier sent by the SS in the preceding CS call setup.
Content-Length	
Value	length of message-body
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:37* - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000/1* [Note 1] - *a=fmtp:* (format) mode-change-capability=2; max-red=220 [Note 1] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 1] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 3] Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2.

C.40 Generic test procedure for MTSI MO speech call for rSRVCC in alerting state - EPS

Test procedure:

1) MO speech is initiated on the UE as a result of receiving information from the lower layers that the CS to PS SRVCC access transfer is initiated. The call is initiated towards the URI of the STI-rSR as received during registration.

2) UE sends an INVITE request to the SS.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with a 183 Session Progress response.

5) SS waits for the UE to send a PRACK request.

6) SS responds to the PRACK request with a 200 OK.

7) UE waits for the SS to send an INFO request.

8) UE responds to the INFO request with a 200 OK.

9) SS waits for the UE to send an INFO request.

10) SS responds to the INVITE request with a 200 OK.

11) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			UE attempt an IMS speech call a result of an initiation of the rSRVCC procedure	
2	→		INVITE	UE sends INVITE with the first SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		183 Session Progress	SS sends an 183 Session Progress
5	→		PRACK	UE acknowledges the 183 Session PRogress
6	←		200 OK	SS sends a 200 OK
7	←		INFO	SS sends INFO request for transfer of incoming early session
8	→		200 OK	UE responds INFO with 200 OK.
8A				Make UE accept the speech call.
9	→		INFO	UE sends INFO request to confirm the call
9A	←		200 OK	SS responds INFO with 200 OK.
10	←		200 OK	SS responds INVITE with 200 OK.
11	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Request-Line	
Request-URI	sip:sti-sr@atcf.visited2.net NOTE: This value was received by the UE in the preceding registration procedure
To	
addr-spec	sip:sti-sr@atcf.visited2.net NOTE: This value was received by the UE in the preceding registration procedure
Message-body	The following SDP types and values. Session description: - v=*0* - *o*=-(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) - *b=RS*: (bandwidth-value) [Note 7] - *b=RR*: (bandwidth-value) [Note 7] Attributes for media: - *a=rtpmap*: (payload type) *AMR-WB/16000* [Note 8] - *a=fmtp*: (format) *mode-change-capability=2; max-red=* (att-field) [Note 9] - *a=rtpmap*: (payload type) *telephone-event*/16000 - *a=fmtp*: (format) - *a=ecn-capable-rtp: leap ect=0* [Note 3] - *a=rtcp-fb:* nack ecn* [Note 3] - *a=rtcp-xr:ecn-sum* [Note 3] - *a=rtcp-rsize* [Note 3] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 4] - *a=a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20 | 1:4FEC_ORDER=FEC_SRTP"* [Note 4] Note 1: At least one "c=" field shall be present. Note 2: Void. Note 3: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 4: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 5: Void Note 6: Void Note 7: The RR value must be greater than 0. The RS value can be any value. Note 8: The AMR channel number shall be "/1" or omitted. Note 9: values from 0 to 220 are allowed

183 Session Progress (Step 4)

Use the default message "183 Session Progress for INVITE" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Recv-Info Info-package-type	*g.3gpp.state-and-event* (cf. RFC 6086 [139] for Recv-Info header)
Feature-Caps feature-param	*+g.3gpp.ti=* (value) Note: The value of this parameter shall be the same as the Transaction Identifier sent by the SS in the preceding CS call setup.
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:37* - *b=RS*: (bandwidth-value) [Note 5] - *b=RR*: (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap*: (payload type) *AMR-WB/16000/1* [Note 1] - *a=fmtp*: (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 1] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 3] Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2.

PRACK (Step 5)

Use the default message “PRACK” in annex A.2.4

INFO (Step 7)

Header/param	Value/remark
Request-Line	
Method	*INFO*
Request-URI	UE’s contact address in SIP URI form, as provided in the Contact header within the INVITE creating the dialog
SIP-Version	*SIP/2.0*
Via	order of the parameters in this header must be like in this table
via-parm1:	
Sent-protocol	*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP
sent-by	IP address and protected server port of SS
via-branch	value starting with ‘*z9hG4bK’* (NOTE 1)
via-parm2:	
sent-protocol	*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP
sent-by	*scscf.3gpp.org*
via-branch	value starting with ‘*z9hG4bK’* (NOTE 1)
From	
addr-spec	*sip:sti-sr@atcf.visited2.net*
tag	tag value corresponding to the SIP URI in the From header
To	
addr-spec	any IMPU within the set of IMPUs on ISIM
tag	tag value corresponding to the SIP URI in the To header
Call-ID	
callid	same as value received in INVITE message
CSeq	
value	value of CSeq sent by the UE within its previous request in the same dialog but increased by one
method	*INFO*
Contact	
addr-spec	*sip:sti-sr@atcf.visited2.net*
Content-Type	
media-type	*application/vnd.3gpp.state-and-event-info+xml*
Max-Forwards	
value	non-zero value
Recv-Info	
Info-package-type	*g.3gpp.state-and-event* (cf. RFC 6086 [139] for Recv-Info header)
Content-Length	
value	length of message-body
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<state-and-event-info>* *<state-info>early</state-info>* *<direction>receiver</direction>* *</state-and-event-info>*

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

INFO (Step 9)

Header/param	Value/remark
Request-Line	
Method	*INFO*
Request-URI	*sip:sti-sr@atcf.visited2.net* NOTE: This value was received by the UE in the preceeding registration procedure.
SIP-Version	*SIP/2.0*
Via	order of the parameters in this header must be like in this table
via-parm1:	
Sent-protocol	*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP
sent-by	IP address and protected server port of SS
via-branch	value starting with '*z9hG4bK'*
via-parm2:	
sent-protocol	*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP
sent-by	*scscf.3gpp.org*
via-branch	value starting with '*z9hG4bK'*
From	
addr-spec	SIP URI of the UE
tag	tag value corresponding to the SIP URI in the From header
To	
addr-spec	*sip:sti-sr@atcf.visited2.net* NOTE: This value was received by the UE in the preceeding registration procedure.
tag	tag value corresponding to the SIP URI in the To header
Call-ID	
callid	same as value received in INVITE message
CSeq	
value	value of CSeq sent by the SS within its previous request in the same dialog but increased by one
method	*INFO*
Contact	
addr-spec	SIP URI of UE
Content-Type	
media-type	*application/vnd.3gpp.state-and-event-info+xml*
Max-Forwards	
value	non-zero value
Recv-Info	
Info-package-type	*g.3gpp.state-and-event* (cf. RFC 6086 [139] for Recv-Info header)
Content-Length	
value	length of message-body
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<state-and-event-info>* *<direction>* initiator*</direction>* *< event>call-accepted</event>* *</state-and-event-info>*

NOTE 1: Branch parameter values sent by SS are different within a test case execution.

C.41 Generic test procedure for MTSI MT speech call for rSRVCC – user reject - EPS

Test procedure:

1) UE sends a CANCEL request to the SS.

2) SS responds to the CANCEL request with a 200 OK.

3) SS responds to the INVITE request with a 487 Request Terminated.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 487 Request Terminated for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		CANCEL	
2	←		200 OK	SS responds CANCEL with 200 OK.
3	←		487 Request Terminated	SS responds INVITE with 487 Request Terminated
4	→		ACK	UE acknowledges.

Specific Message Contents

CANCEL (Step 1)

Use the default message "CANCEL" in annex A.2.15 with the following exceptions:

Header/param	Value/Remark
Reason	
reason-value	*SIP; cause=486;text= "Busy Here"*

487 Request Terminated (Step 3)

Use the default message "487 Request Terminated" in annex A.2.16

ACK (Step 4)

Use the default message "ACK" in annex A.2.7

C.42 Generic Test Procedure – UE receiving the ATGW information for CS to PS SRVCC - EPS

The generic test procedure:

1. The UE waits for the SS to send a MESSAGE including SDP details to be used for CS to PS SRVCC.
2. The UE responds to the MESSAGE with a 200 OK response
3. The SS waits for the UE to send a MESSAGE including SDP details to be used for CS to PS SRVCC.
4. The SS responds to the MESSAGE with a 200 OK response

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		MESSAGE	The SS sends MESSAGE indicating SDP details.
2	→		200 OK	The UE responds with 200 OK.
3	→		MESSAGE	The UE sends MESSAGE indicating SDP details.
4	←		200 OK	The SS responds with 200 OK.

Specific Message Contents

NOTE: The default message contents in annex A are used with the following exceptions:

MESSAGE (Step 1)

Use the default message "MESSAGE UE receiving the ATGW information for CS to PS SRVCC" in annex A.8.1 with following exception:

Header/param	Value/Remark
Message-body	Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN IP4 0.0.0.0* [NOTE 1] - *c=IN IP6 dfgrrgr.invalid* [NOTE 2] - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio 9 RTP/AVP 97 99* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Note 1: In case IPv4 is used Note 2: In case IPv6 is used

200 OK (Step 2)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with condition A5 “Any response sent by the UE within a dialog”.

MESSAGE (Step 3)

Use the default message "MESSAGE UE providing information for CS to PS SRVCC" in annex A.8.2 with following exception:

Header/param	Value/Remark
Message-body	Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked Note 3: Parameters for the AMR codec are not checked

200 OK (Step 4)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with condition A5 “Any response sent by the UE within a dialog”.

C.43 Generic Test Procedure for UE receiving SIP REFER request for transfer of additional CS to PS call - EPS

Test procedure:

1. The UE waits for the SS to send a REFER request in dialog of INVITE to STI-rSR for transfer of 2nd call
2. The UE responds to the REFER with a 200 OK response
3. The UE sends INVITE request for transfer of additional call
4. The SS responds to the INVITE with a 200 OK response
5. The UE sends ACK for receipt of 200 OK

Expected sequence:

Step	Direction UE	Direction SS	Message	Comment
1	←		REFER	The SS sends REFER request
2	→		200 OK	The UE responds with 200 OK.
3	→		INVITE	The UE sends INVITE for transfer of additional call
4	←		200 OK	The SS responds with 200 OK.
5	→		ACK	UE acknowledges the receipt of 200 OK for INVITE

Specific message contents:

REFER (Step 1)

Use the default message "MT REFER" in annex A.2.12 with the following exceptions:

Header/param	Value/remark
Request-URI	SS sends REFER request in the dialog of the INVITE to STI-rSR for transfer of second call
Refer-To	
addr-spec	SIP or Tel URI of the transfer target
To	
addr-spec	SIP URI of the UE which shall be the same URI as used for UE in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred
tag	no tag given
CSeq	
value	any value

200 OK for REFER (Step 2)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Refer-Sub	
referSubValue	false

INVITE (Step 3)

Use the default message "INVITE for MO Call" in annex A.2.1, with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v*=0 - *o*=(username) (sess-id) (sess-version) *IN (addrtype)* (unicast-address for UE) - *c*=*IN* (addrtype) (connection-address for UE) [Note 1] - *s*=(session name) - *b*=*AS:* (bandwidth-value) Time description: - *t*=(start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 6] - *b=RR:* (bandwidth-value) [Note 6] Attributes for media: - *a=rtpmap*:(payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 4] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp*:(format) Attributes for preconditions: - *a=curr:qos local sendonly* - *a=curr:qos remote none* - *a=des:qos mandatory local sendonly* - *a=des:qos optional remote sendonly* Note 1: At least one "c=" field shall be present. Note 2: Void Note 3: The AMR channel number shall be “/1” or omitted. Note 4: Values from 0 to 220 are allowed Note 5: A rate may be added to the “telephone-event” separated by “/” (e.g. "telephone-event/8000") Note 6: The RR value must be greater than 0. The RS value can be any value.

200 OK for INVITE (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Message-body	SDP body of the 200 OK response copied from the received INVITE but modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and transport port on "m=" lines changed to indicate to which IP address and port the UE should send the media; and In case of Call Hold: - "sendonly" direction attribute inverted to "recvonly". Note that this applies to “a=sendonly” direction attributes only, not to the direction tags found in preconditions.

C.44 Generic test procedure for setting up MTSI MO speech call - EVS - EPS

Test procedure:

1- 13) See generic test procedure C.21.

Expected sequence:

See generic test procedure C.21

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 9] - *b=RR:* (bandwidth-value) [Note 9] Attributes for media: - *a=rtpmap:* (payload type) *EVS/16000* [Note 5, 10] - *a=fmtp:* (format) *max-red=* (att-field) [Note 6, 7] - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 5, 10] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 6, 8] - *a=rtpmap:* (payload type) *telephone-event/16000* - *a=fmtp:* (format) - *a=rtpmap:* (payload type) *AMR/8000* [Note 5, 10] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 6, 8] - *a=rtpmap:* (payload type) *telephone-event/8000* - *a=fmtp:* (format) - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=rtcp-rsize* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 3] - *a=a=crypto:1* *AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20* | *1:4FEC_ORDER=FEC_SRTP"* [Note 3] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: Void Note 5: The channel number shall be "/1" or omitted. Note 6: Values from 0 to 220 are allowed in the att-field. Note 7: The parameters dtx, dtx-recv and evs-mode-switch shall not be present. Note 8: The parameters mode-set, mode-change-period, mode-change-neighbor, crc, robust-sorting and interleaving shall not be present. Note 9: The RR value must be greater than 0. The RS value can be any value. Note 10: The ordering of payload types shall be as listed, i.e., EVS before AMR-WB before AMR.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:65* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:65* - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *EVS/16000/1* [Note 1] - *a=fmtp:* (format) *max-red=220* [Note 1, 8, 9] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 1] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 3] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The values for fmt, payload type and format are copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: Transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2. Note 6: Void Note 7: Void Note 8: All present br, br-send and br-recv parameter=value pairs are copied from step 2. Note 9: bw, bw-send and bw-recv parameter are copied from bw at step 2.

PRACK (Step 5)

Use the default message “PRACK” in annex A.2.4 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *EVS/16000* [Note 3] [Note 5] - *a=fmtp:* (format) [Note 3][Note 4] - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the codec are not checked Note 5: The channel number shall be “/1” or omitted.

200 OK for PRACK (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 OK response copied from the received PRACK and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

UPDATE (Step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Require	Same contents as specified in step 5.
Message-body	Same contents as specified in step 5.

200 OK for UPDATE (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition* (shall be present if SDP message-body present)
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented. Attributes for preconditions: - *a=curr:qos remote sendrecv*

180 Ringing (Step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6 applying condition A3 (Response sent reliably).

C.45 Generic test procedure for setting up MTSI MT speech call - EVS - EPS

Test procedure

1-15) See generic test procedure C.11.

Expected sequence

See generic test procedure C.11.

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:65* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 96 97 98 99 100* - *b=AS:65* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:96 EVS/16000/1* - *a=fmtp:96 br=8-48; bw=nb-fb; max-red=220* - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap:98 telephone-event/16000* - *a=fmtp:98 0-15* - *a=rtpmap: 99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=rtpmap: 100 telephone-event/8000* - *a=fmtp: 100 0-15* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	 Not checked
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *EVS/16000* [Note 3] - *a=fmtp:*(format) *br*= (att-field)*; bw*= (att-field) [Note 3] Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: Void Note 3: The value for fmt, payload type and format is not checked

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:65* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 96* - *b=AS:65* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:96 EVS/16000/1* - *a=fmtp:96 br=* (att-field) *bw=* (att-field)*; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 2] - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* [Note 3] Note 1: The br and bw values are taken from step 4 Note 2: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local. Note 3: “optional” as strength tag of remote leg intentionally deviates from other MT scenarios in order to improve test coverage.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 4] - *s*=(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *EVS/16000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The values for fmt, payload type and format are not checked. Note 3: Parameters for the codec are not checked. Note 4: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

180 Ringing (Step 9)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header not present
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body 0
Message-body	Not present

C.46 Generic test procedure for IMS Re-Registration

The generic test procedure for IMS re-registration

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The SS receives REGISTER from the UE
2	←		200 OK	The SS responds with 200 OK.

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1 with condition A2 "Subsequent REGISTER sent over security associations".

C.47 Generic Test Procedure for NG eCall setup and MSD Update

Test procedure:

1) SS waits for UE to send an INVITE request with initial MSD.
2) SS responds to the INVITE request with a 200 OK response.
3) UE responds to the 200 OK with ACK.
4) SS sends a SIP INFO to request UE for a MSD update.
5) UE responds to the MSD update request with 200 OK response.
6) SS waits for UE to send a SIP INFO with updated MSD.
7) The SS responds to the SIP INFO with a 200 OK response.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with initial MSD.
2	←		200 OK	SS responds INVITE with 200 OK.
3	→		ACK	UE responds ACK for 200 OK.
4	←		SIP INFO	SS sends SIP INFO to request MSD update.
5	→		200 OK	UE responds SIP INFO with 200 OK.
6	→		SIP INFO	UE sends SIP INFO with MSD update.
7	←		200 OK	SS responds SIP INFO with 200 OK.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MO Call" in annex A.2.1 with the following inclusion along with the applicable message body of default message:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - c=IN (addrtype) (connection-address for UE) [Note 1] Time description: - t= (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec (AMR/8000 and/or AMR-WB/16000) shall be present in the media attributes, optionally including channel number "/1".

200 OK for INVITE (Step 2)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following inclusion along with the applicable message body of default message:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0* 0 Media description: - *m=audio* (transport port) RTP/AVP (fmt) [Note 1] - *b=AS:37* - *b=RS:0* - *b=RR:0* Attributes for media: - *a=rtpmap*: (payload type) *AMR/8000/1 or AMR-WB/16000/1* [Note 1] [Note2] - *a=fmtp*: (format) *mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Note 1: The value for fmt, payload type and format is copied from step 1. Note 2: If UE included AMR-WB/16000 in step 1, SS uses AMR-WB/16000/1. Otherwise SS uses AMR/8000/1.

INFO (Step 4)

Use the default message "INFO for MT" in annex A.2.20.

INFO (Step 6)

Use the default message "INFO for MO" in annex A.2.19.

C.48 to C.51 Void

Annex D (Informative): Example values for certain IXIT parameters

This table contains syntactically correct example values for a number of headers and parameters that may be used as such by SS when sending downlink messages and checking that the uplink messages would contain the same values. These values will be defined as IXIT.

IMS registration parameters from ISIM application px_IMS_HomeDomainName 3gpp.org px_IMS_PublicUserIdentity1 sip:localuser@3gpp.org px_IMS_PrivateUserIdentity privateuser@3gpp.org	
IMS registration parameters derived from IMSI when using USIM application IMSI 12345611223344 home domain name ims.mnc123.mcc456.3gppnetwork.org public user identity sip:12345611223344@ ims.mnc123.mcc456.3gppnetwork.org private user identity 12345611223344@ ims.mnc123.mcc456.3gppnetwork.org	TS 23.003 [32]

Annex E (normative): Test ISIM Parameters

E.1 Introduction

This annex defines the default parameters to be programmed into the elementary files of the ISIM application.

Access conditions, data items and coding for the EFs for IMS session are defined in clause 4 of 3GPP TS 31.103 [31.103].

The parameters to be programmed into the elementary files for the USIM application are defined in clause 8.3 of 3GPP TS 34.108 [34.108].

E.2 Definitions

"Test ISIM card":

A ISIM card supporting the test algorithm for authentication defined in clause 8.1.2 of [34.108], programmed with the parameters defined in this annex and clause 8 of 3GPP TS 34.108 [34.108].

E.3 Default settings for the Elementary Files (EFs)

The format and coding of elementary files of the ISIM/USIM are defined in 3GPP TS 31.101 [31.101] and 3GPP TS 31.103 [31.103].

This annex defines the default parameters to be programmed into each elementary file of the ISIM/USIM.

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

E.3.1 Contents of the EFs at the MF level

The contents of the EFs at the MF level are defined in clause 8.3.1 in 3GPP TS 34.108 [34.108].

E.3.2 Contents of files at the ISIM ADF (Application DF) level

E.3.2.1 EF_{IMPI} (IMS private user identity)

As defined in TS 31.121 [113].

E.3.2.2 EF_{DOMAIN} (Home Network Domain Name)

As defined in TS 31.121 [113].

E.3.2.3 EF_{IMPU} (IMS public user identity)

As defined in TS 31.121 [113], but with MCC and MNC values aligned to the HPLMN of the EF IMSI in the USIM ADF according to clause 8.3.2.2 in 3GPP TS 34.108 [40].

E.3.2.4 EF_{AD} (Administrative Data)

This EF is programmed as defined in clause 8.3.2.18 in 3GPP TS 34.108 [40].

E.3.2.5 EF_{ARR} (Access Rule Reference)

The programming of this EF is a test house option.

E.3.2.6 EF_{IST} (ISIM Service Table)

As defined in TS 31.121 [113].

E.3.2.7 $EF_{P\text{-}CSCF}$ (P-CSCF Address)

As defined in TS 31.121 [113].

E.3.2.8 EF_{GBABP} (GBA Bootstrapping parameters)

The programming of this EF is a test house option.

E.3.2.9 EF_{GBANL} (GBA NAF List)

The programming of this EF is a test house option.

E.3.2.10 EF_{NAFKCA} (NAF Key Centre Address)

The programming of this EF is a test house option.

E.3.2.11 EF_{SMS} (Short messages)

As defined in TS 31.121 [113].

E.3.2.12 EF_{SMSS} (SMS status)

As defined in TS 31.121 [113].

E.3.2.13 EF_{SMSR} (Short message status reports)

As defined in TS 31.121 [113].

E.3.2.14 EF_{SMSP} (Short message service parameters) As defined in TS 31.121 [113].

E.3.2.15 $EF_{PSISMSC}$ (Public Service Identity of the SM-SC)

As defined in TS 31.121 [113].

This EF is either a SIP URI or a TEL URI and must be present on the ISIM if ISIM is used or on the USIM if USIM is used.

Annex F (normative): Generic Requirements for MTSI Supplementary Services

This Annex contains references to such generic requirements for IMS Multimedia Telephony Supplementary Services which apply to multiple test cases. These references are to the 3GPP documents, most of which were earlier annexes of TS 24.173 [65].

F.1 XCAP over Ut interface

The generic UE requirements for XCAP over Ut interface are specified in 3GPP TS 24.623 [105] clauses 4, 5.1, 5.2.1, 5.3.1 and 6.

The generic UE requirements for XCAP authentication over Ut interface are specified in 3GPP 24.623 [105] clause 5.2.1.1 and TS 33.220 clauses 4 and 4.3.1

[TS 24.623 clause 5.2.1.1]:

For systems where Generic Authentication Architecture is used, the UE shall support the authentication mechanisms specified in 3GPP TS 33.222 and 3GPP TS 24.109.

For systems where Generic Authentication Architecture is not used, the UE shall support RFC 2617 and RFC 2246 according to ETSI TS 183 038.

…

[TS 33.220 clause 4]:

The 3GPP authentication infrastructure, including the 3GPP Authentication Centre (AuC), the USIM or the ISIM, and the 3GPP AKA protocol run between them, is a very valuable asset of 3GPP operators. It has been recognised that this infrastructure could be leveraged to enable application functions in the network and on the user side to establish shared keys. Therefore, 3GPP can provide the "bootstrapping of application security" to authenticate the subscriber by defining a Generic Bootstrapping Architecture (GBA) based on AKA protocol.

…

[TS 33.220 clause 4.3.1]:

The reference point Ub is between the UE and the BSF. Reference point Ub provides mutual authentication between the UE and the BSF. It allows the UE to bootstrap the session keys based on 3GPP AKA infrastructure.

The HTTP Digest AKA protocol, which is specified in RFC 3310, is used on the reference point Ub. It is based on the 3GPP AKA TS 33.102 protocol. The interface to the USIM is as specified in TS 31.102 and to the ISIM is as specified in TS 31.103.

F.2 Originating Identification Presentation (OIP) / Originating Identification Restriction (OIR)

The UE requirements for Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) are specified in 3GPP TS 24.607 [102] clauses 4.2, 4.5.0, 4.5.1, 4.5.2.1, 4.5.2.12 and 4.10.

F.3 Terminating Identification Presentation (TIP) / Terminating Identification Restriction (TIR)

The UE requirements for Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) are specified in 3GPP TS 24.608 [103] clauses 4.2, 4.5.0, 4.5.1, 4.5.2.1, 4.5.2.12 and 4.9.

F.4 Communication Diversion (CDIV)

The UE requirements for Communication Diversion (CDIV) are specified in 3GPP TS 24.604 [106] clauses 4.2, 4.5.0, 4.5.1, 4.5.2.1, 4.5.2.15, 4.5.2.16 and 4.9.

F.5 Communication Barring (CB)

The UE requirements for Communication Barring (CB) are specified in 3GPP TS 24.611 [101] clauses 4.2, 4.5.0, 4.5.1, 4.5.2.1, 4.5.2.13 and 4.9.

Annex G (normative): IP-Connectivity Access Network specific test cases when using the EPC via WLAN to access IM CN subsystem

G.1 Scope

The present annex defines IP-CAN specific test cases for a call control protocol for use in the IM CN subsystem based on the Session Initiation Protocol (SIP) and the associated Session Description Protocol (SDP) where the IP-CAN is the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN).

G.2 to G.7

G.8 Registration / WLAN

G.8.1 Initial registration / WLAN

G.8.1.1 Definition

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing the registration event package for the registered default public user identity using WLAN access.

G.8.1.2 Conformance requirement

As described in clause 8.1.2.

G.8.1.3 Test purpose

As described in clause 8.1.3

G.8.1.4 Method of test

As described in generic procedure C.2c.

G.8.1.5 Test requirements

As described in clause 8.1.5

G.9 to G.11

G.12 Call Control

G.12.1 MO MTSI speech call / WLAN

G.12.1.1 Definition

Test to verify that the UE correctly setup a IMS mobile originated voice call over WLAN and release it. This process is described in 3GPP TS 24.229 [10], clauses 5.1.2A.1, 5.1.3 and 6.1, and TS 26.114 [66], clauses 5.2.1, 6.2.2.1, 6.2.5 and 7.3.1.

G.12.1.2 Conformance requirement

As described in clause 12.12.2 and the following:

[Rel-13, TS 24.229, clause R.2.2.1]

Prior to communication with the IM CN subsystem:

…

a) the UE establishes an IP-CAN bearer for SIP signalling as follows:

…

b) the UE shall acquire a P-CSCF address(es).

…

The methods for P-CSCF discovery are:

…

IV. Obtain P-CSCF address(es) using signalling for access to the EPC via WLAN.

If the UE attaches to the EPC via S2b using untrusted WLAN IP access, the UE shall request P-CSCF IPv4 address(es), P-CSCF IPv6 address(es) or both using the P_CSCF_IP4_ADDRESS attribute, the P_CSCF_IP6_ADDRESS attribute or both in the CFG_REQUEST configuration payload as described in 3GPP TS 24.302 [8U]. The network can provide the UE with the P-CSCF IPv4 address(es), P-CSCF IPv6 address(es) or both using the P_CSCF_IP4_ADDRESS attribute, the P_CSCF_IP6_ADDRESS attribute or both in the CFG_REPLY configuration payload as described in 3GPP TS 24.302 [8U]. If the UE receives multiple P-CSCF IPv4 or IPv6 addresses, the UE shall assume that the list is ordered top-down with the first P-CSCF address within the CFG_REPLY configuration payload as the P-CSCF address having the highest preference and the last P-CSCF address within the CFG_REPLY configuration payload as the P-CSCF address having the lowest preference.

G.12.1.3 Test purpose

As described in clause 12.12.3.

G.12.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN). The UE has registered to IMS according the procedures C.2c.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.21a	MTSI MO speech call.
9				Void
10			The UE is triggered by MMI to release the call	
11	→		BYE	The UE releases the call with BYE
12	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

None.

G.12.1.5 Test requirements

The UE shall send requests and responses as described in clause G.12.1.4.

G.12.2 MT MTSI speech call / WLAN

G.12.2.1 Definition

Test to verify that the UE correctly setup a IMS mobile terminated voice call over WLAN and release it. This process is described in 3GPP TS 24.229 [10], clauses 5.1.4.1, 6.1.1 and 6.1.3.

G.12.2.2 Conformance requirement

As described in clause 12.13.2 and the following:

[Rel-13, TS 24.229, clause R.2.2.1]

Prior to communication with the IM CN subsystem:

…

a) the UE establishes an IP-CAN bearer for SIP signalling as follows:

…

b) the UE shall acquire a P-CSCF address(es).

…

The methods for P-CSCF discovery are:

…

IV. Obtain P-CSCF address(es) using signalling for access to the EPC via WLAN.

If the UE attaches to the EPC via S2b using untrusted WLAN IP access, the UE shall request P-CSCF IPv4 address(es), P-CSCF IPv6 address(es) or both using the P_CSCF_IP4_ADDRESS attribute, the P_CSCF_IP6_ADDRESS attribute or both in the CFG_REQUEST configuration payload as described in 3GPP TS 24.302 [8U]. The network can provide the UE with the P-CSCF IPv4 address(es), P-CSCF IPv6 address(es) or both using the P_CSCF_IP4_ADDRESS attribute, the P_CSCF_IP6_ADDRESS attribute or both in the CFG_REPLY configuration payload as described in 3GPP TS 24.302 [8U]. If the UE receives multiple P-CSCF IPv4 or IPv6 addresses, the UE shall assume that the list is ordered top-down with the first P-CSCF address within the CFG_REPLY configuration payload as the P-CSCF address having the highest preference and the last P-CSCF address within the CFG_REPLY configuration payload as the P-CSCF address having the lowest preference.

G.12.2.3 Test purpose

As described in clause 12.13.3.

G.12.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN). The UE has registered to IMS according the procedures C.2c.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-7			Steps defined in annex C.11a	MT MTSI speech call over WLAN Access.
8-9				Void
10			The SS is triggered to release the call	
11	←		BYE	The SS releases the call with BYE
12	→		200 OK	The UE sends 200 OK for BYE

Specific Message Content

None.

G.12.2.5 Test requirements

The UE shall send requests and responses as described in clause G.12.2.4.

G.12.3 MO MTSI video call / WLAN

G.12.3.1 Definition

Test to verify that the UE correctly performs IMS mobile originated video call setup and release when using IMS Multimedia Telephony with preconditions, using WLAN access. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

G.12.3.2 Conformance requirement

As described in clause 12.21.2 and the following:

[Rel-13, TS 24.229, clause R.2.2.1]

Prior to communication with the IM CN subsystem:

…

a) the UE establishes an IP-CAN bearer for SIP signalling as follows:

…

b) the UE shall acquire a P-CSCF address(es).

…

The methods for P-CSCF discovery are:

…

IV. Obtain P-CSCF address(es) using signalling for access to the EPC via WLAN.

If the UE attaches to the EPC via S2b using untrusted WLAN IP access, the UE shall request P-CSCF IPv4 address(es), P-CSCF IPv6 address(es) or both using the P_CSCF_IP4_ADDRESS attribute, the P_CSCF_IP6_ADDRESS attribute or both in the CFG_REQUEST configuration payload as described in 3GPP TS 24.302 [8U]. The network can provide the UE with the P-CSCF IPv4 address(es), P-CSCF IPv6 address(es) or both using the P_CSCF_IP4_ADDRESS attribute, the P_CSCF_IP6_ADDRESS attribute or both in the CFG_REPLY configuration payload as described in 3GPP TS 24.302 [8U]. If the UE receives multiple P-CSCF IPv4 or IPv6 addresses, the UE shall assume that the list is ordered top-down with the first P-CSCF address within the CFG_REPLY configuration payload as the P-CSCF address having the highest preference and the last P-CSCF address within the CFG_REPLY configuration payload as the P-CSCF address having the lowest preference.

G.12.3.3 Test purpose

As described in clause 12.21.3.

G.12.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN). The UE has registered to IMS according to the procedures in Annex C.2c.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.25a	MTSI MO video call.
9				Make the UE release the IMS call
10	→		BYE	The UE releases the call with BYE
11	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Steps 1 - 8 as specified in annex C.25a.

BYE (Step 10)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 11)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

G.12.3.5 Test requirements

The UE shall send requests and responses as described in clause G.12.3.4.

G.12.4 MT MTSI video call / WLAN

G.12.4.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated video call setup when using IMS Multimedia Telephony, using WLAN access. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

G.12.4.2 Conformance requirement

As described in clause 12.21.2 and the following:

[Rel-13, TS 24.229, clause R.2.2.1]

Prior to communication with the IM CN subsystem:

…

a) the UE establishes an IP-CAN bearer for SIP signalling as follows:

…

b) the UE shall acquire a P-CSCF address(es).

…

The methods for P-CSCF discovery are:

…

IV. Obtain P-CSCF address(es) using signalling for access to the EPC via WLAN.

If the UE attaches to the EPC via S2b using untrusted WLAN IP access, the UE shall request P-CSCF IPv4 address(es), P-CSCF IPv6 address(es) or both using the P_CSCF_IP4_ADDRESS attribute, the P_CSCF_IP6_ADDRESS attribute or both in the CFG_REQUEST configuration payload as described in 3GPP TS 24.302 [8U]. The network can provide the UE with the P-CSCF IPv4 address(es), P-CSCF IPv6 address(es) or both using the P_CSCF_IP4_ADDRESS attribute, the P_CSCF_IP6_ADDRESS attribute or both in the CFG_REPLY configuration payload as described in 3GPP TS 24.302 [8U]. If the UE receives multiple P-CSCF IPv4 or IPv6 addresses, the UE shall assume that the list is ordered top-down with the first P-CSCF address within the CFG_REPLY configuration payload as the P-CSCF address having the highest preference and the last P-CSCF address within the CFG_REPLY configuration payload as the P-CSCF address having the lowest preference.

G.12.4.3 Test purpose

As described in clause 12.21.3.

G.12.4.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN). The UE has registered to IMS according to the procedures in Annex C.2c.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-7			Steps defined in annex C.26a	MTSI MT video call.
8	←		BYE	The SS sends BYE to release the call.
9	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition “IMS security“ or “GIBA” when applicable

Specific Message Content

None.

G.12.4.5 Test requirements

The UE shall send requests and responses as described in clause G.12.4.4.

G.13 to G.14

G.15 Supplementary Services

G.15.1 Originating Identification Presentation / WLAN

G.15.1.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Originating Identification Presentation. This process is described in 3GPP TS 24.607 [102].

G.15.1.2 Conformance requirement

As described in clause 15.1.2.

G.15.1.3 Test purpose

As described in clause 15.1.3.

G.15.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Originating Identification Presentation, at step 7 deactivation of Originating Identification Presentation is respectively triggered at the UE.

G.15.1.5 Test requirements

As described in clause 15.1.5.

G.15.2 Originating Identification Restriction / WLAN

G.15.2.1 Definition

Test to verify that the UE correctly invokes the IMS Multimedia Telephony Originating Identification Restriction. This process is described in 3GPP TS 24.607 [102].

G.15.2.2 Conformance requirement

As described in clause 15.2a.2.

G.15.2.3 Test purpose

As described in clause 15.2a.3.

G.15.2.4 Method of test

Initial conditions

Same as clause G.12.1 with the following addition:

The UE is configured for Originating Identification Restriction

Test procedure

As described in clause 15.2a.4, steps 1-14. Except, steps 2-13 replaced by steps 1-8 in C.21a.

G.15.2.5 Test requirements

As described in clause 15.2a.5.

G.15.3 Terminating Identification Presentation / WLAN

G.15.3.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Terminating Identification Presentation. This process is described in 3GPP TS 24.608 [103].

G.15.3.2 Conformance requirement

As described in clause 15.3.2.

G.15.3.3 Test purpose

As described in clause 15.3.3.

G.15.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Terminating Identification Presentation, at step 7 deactivation of Terminating Identification Presentation is respectively triggered at the UE.

G.15.3.5 Test requirements

As described in clause 15.3.5.

G.15.4 Terminating Identification Restriction / WLAN

G.15.4.1 Definition

Test to verify that the UE correctly invokes the IMS Multimedia Telephony Terminating Identification Restriction. This process is described in 3GPP TS 24.608 [103].

G.15.4.2 Conformance requirement

As described in clause 15.4a.2.

G.15.4.3 Test purpose

As described in clause 15.4a.3.

G.15.4.4 Method of test

Initial conditions

Same as clause G.12.2 with the following addition:

The UE is configured for Terminating Identification Restriction

Test procedure

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-5			Steps 1-5 defined in annex C.11a	MTSI MT speech call.
6				Make UE accept the speech offer with Terminating Identification Restriction
7-8			Steps 6-7 defined in annex C.11a	MTSI MT speech call.

Specific Message Contents

183 Session Progress (Step 2A)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark	Reference
Privacy	*id*	RFC 3323 [135] RFC 3325 [89]

180 Ringing (Step 3)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following exceptions:

Header/param	Value/remark	Reference
Privacy	*id*	RFC 3323 [135] RFC 3325 [136]

200 Ok (Step 7)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark	Reference
Privacy	*id*	RFC 3323 [135] RFC 3325 [136]

G.15.4.5 Test requirements

The UE shall send requests and responses as described in clause G.15.4.4.

G.15.5 Communication forwarding unconditional / WLAN

G.15.5.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding unconditional. This process is described in 3GPP TS 24.604 [106].

G.15.5.2 Conformance requirement

As described in clause 15.5.2.

G.15.5.3 Test purpose

As described in clause 15.5.3.

G.15.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding unconditional, at step 7 deactivation of Communication Forwarding unconditional is respectively triggered at the UE.

G.15.5.5 Test requirements

As described in clause 15.5.5.

G.15.6 Communication forwarding on non Reply: activation / WLAN

G.15.6.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user does not answer to the phone. This process is described in 3GPP TS 24.604 [106].

G.15.6.2 Conformance requirement

As described in clause 15.7.2.

G.15.6.3 Test purpose

As described in clause 15.7.3.

G.15.6.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding on non Reply, at step 7 deactivation of Communication Forwarding on non Reply is respectively triggered at the UE.

G.15.6.5 Test requirements

As described in clause 15.7.5

G.15.7 Communication forwarding on non reply: MO call initiation / WLAN

G.15.7.1 Definition

Test to verify that the MTSI MO UE correctly handles session setup where call is being forwarded due to no reply. This process is described in 3GPP TS 24.604 [106], clauses 4.2.1, 4.5.2.1 and A.1.3 and 3GPP TS 24.229 [10], clause 9.2.3

G.15.7.2 Conformance requirement

As described in clause 15.8.2.

G.15.7.3 Test purpose

As described in clause 15.8.3.

G.15.7.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS according the procedure C.2c.

Test procedure

1-6) Steps 1-6, procedure C.21a.

7) SS responds to the INVITE with a valid 181 Call Is Being Forwarded response (simulate the UE to which call was forwarded)

8) SS responds to the INVITE request with 180 Ringing response.

9) As the 180 Ringing response was sent reliably, UE sends a PRACK request.

10) SS responds to PRACK with 200 OK.

11) SS responds to the INVITE request with a 200 OK response.

12) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

13) Call is released on the UE. SS waits the UE to send a BYE request.

14) SS responds to the BYE request with a 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-6			Steps 1-6 as defined in Annex C.21a	
7	←		181 Call is being forwarded	SS sends 181 response to indicate that call forwarding has been started as the user did not answer to the phone
8	←		180 Ringing	The SS sends 180 Ringing response to the UE
9	→		PRACK	UE acknowledges the receipt of 180 response by sending PRACK.
10	←		200 OK	The SS responds PRACK with 200 OK.
11	←		200 OK	The SS responds INVITE with 200 OK to indicate that the virtual remote UE had answered the call
12	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
13	→		BYE	The UE releases the call with BYE
14	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

180 Ringing (Step 8)

Use the default message "180 Ringing for INVITE" in annex A.2.6 applying condition A3 (Response sent reliably) and with the following exceptions:

Header/param	Value/remark
To	
tag	different tag must be used than the one used in steps 3-9 as this response is now from another UE and belongs to another dialog instance. Note that this new tag must be used within the rest of the steps (10-17) in this test case instead of the tag used within steps 3-9.
Contact	
addr-spec	different URI must be used than the one used in step 3 as this is supposed now to represent another UE to which the call is being forwarded.. Note that this new Contact must be used within the rest of the steps (13-14) in this test case.
History-Info	
hi-targeted-to-uri	Same value as in the 181 response of step 7
hi-index	Same value as in the 181 response of step 7
Require	
option-tag	*precondition*
Content-Type	
media-type	*application/sdp*
Message-body	Same contents as specified in step 4 annex C.21a except for o-line: *o=- 22222222 22222222 IN* (addrtype) (unicast-address for new remote UE).

200 OK (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	Same value as in the 180 response of step 8
History-Info	
hi-targeted-to-uri	Same value as in the 181 response of step 7
hi-index	Same value as in the 181 response of step 7

G.15.7.5 Test requirements

The UE shall send requests and responses as described in clause G.15.7.4.

G.15.8 Communication Forwarding on Busy / WLAN

G.15.8.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is busy. This process is described in 3GPP TS 24.604 [106].

G.15.8.2 Conformance requirement

As described in clause 15.9.2.

G.15.8.3 Test purpose

As described in clause 15.9.3.

G.15.8.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding on Busy, at step 7 deactivation of Communication Forwarding on Busy is respectively triggered at the UE.

G.15.8.5 Test requirements

As described in clause 15.9.5

G.15.9 Communication Forwarding on Not logged-in / WLAN

G.15.9.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is not registered to IMS service. This process is described in 3GPP TS 24.604 [106].

G.15.9.2 Conformance requirement

As described in clause 15.10.2.

G.15.9.3 Test purpose

As described in clause 15.10.3.

G.15.9.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding on not logged-in, at step 7 deactivation of Communication Forwarding on Not logged-in is respectively triggered at the UE.

G.15.9.5 Test requirements

As described in clause 15.10.5

G.15.10 Communication Forwarding on Not reachable / WLAN

G.15.10.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is not reachable. This process is described in 3GPP TS 24.604 [106].

G.15.10.2 Conformance requirement

As described in clause 15.10a.1.

G.15.10.3 Test purpose

As described in clause 15.10a.3.

G.15.10.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding on Not reachable;

At step 5b, SS delivers a simservs document as specified in TS 24.604 [106] cl 4.9, including a non-empty rule set. Specifically, the SS includes the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<simservs
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
xmlns:cp="urn:ietf:params:xml:ns:common-policy"
xmlns:ocp="urn:oma:xml:xdm:common-policy">
   <communication-diversion active="true">
         <cp:ruleset>
      <cp:rule id="rule1">
               <cp:conditions>
                   <not-reachable/>
                   <rule-deactivated/>
               </cp:conditions>

               <cp:actions>
                   <forward-to>
                       <target>
                          px_XCAP_TargetUri
                       </target>
                       <notify-caller>true</notify-caller>
                   </forward-to>
               </cp:actions>
           </cp:rule>
         </cp:ruleset>
   </communication-diversion>
</simservs>
```

At step 7 deactivation of Communication Forwarding on Not reachable is respectively triggered at the UE.

G.15.10.5 Test requirements

As described in clause 15.10a.5

G.15.11 MO Call Hold without announcement / WLAN

G.15.11.1 Definition

Test to verify that the UE correctly performs IMS mobile originated call hold and resume. This process is described in 3GPP TS 24.610 [108].

G.15.11.2 Conformance requirement

As described in clause 15.11.2.

G.15.11.3 Test purpose

As described in clause 15.11.3.

G.15.11.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MO call according the procedures C.2c and C.21a.

Test procedure

As described in clause 15.11.4.

G.15.11.5 Test requirements

As described in clause 15.11.5.

G.15.12 MT Call Hold without announcement / WLAN

G.15.12.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated call hold and resume. This process is described in 3GPP TS 24.610 [108].

G.15.12.2 Conformance requirement

As described in clause 15.12.2.

G.15.12.3 Test purpose

As described in clause 15.12.3.

G.15.12.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MO call according the procedures C.2c and C.21a.

Test procedure

As described in clause 15.12.4.

G.15.12.5 Test requirements

As described in clause 15.12.5.

G.15.13 MO video Call Hold without announcement / WLAN

G.15.13.1 Definition

Test to verify that the UE correctly performs IMS mobile originated video call hold and resume. This process is described in 3GPP TS 24.610 [108].

G.15.13.2 Conformance requirement

As described in clause 15.11a.2.

G.15.13.3 Test purpose

As described in clause 15.11a.3.

G.15.13.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MO video call according the procedures C.2c and C.25a.

Test procedure

As described in clause 15.11a.4.

G.15.13.5 Test requirements

As described in clause 15.11a.5.

G.15.14 MT video Call Hold without announcement / WLAN

G.15.14.1 Definition

Test to verify that the UE correctly performs IMS mobile terminated video call hold and resume. This process is described in 3GPP TS 24.610 [108].

G.15.14.2 Conformance requirement

As described in clause 15.12a.2.

G.15.14.3 Test purpose

As described in clause 15.12a.3.

G.15.14.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MO video call according the procedures C.2c and C.25a.

Test procedure

As described in clause 15.12a.4.

G.15.14.5 Test requirements

As described in clause 15.12a.5.

G.15.15 Incoming Communication Barring while roaming / WLAN

G.15.15.1 Definition

Test to verify that the UE activates and deactivates the "IMS Multimedia Telephony Communication Barring for incoming calls while the user is roaming" supplementary service while camping on HPLMN. This process is described in 3GPP TS 24.611 [101].

G.15.15.2 Conformance requirement

As described in clause 15.14a.2.

G.15.15.3 Test purpose

As described in clause 15.14a.3.

G.15.15.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Incoming Communication Barring, at step 7 deactivation of Incoming Communication Barring is respectively triggered at the UE.

G.15.15.5 Test requirements

As described in clause 15.14a.5

G.15.16 Outgoing Communication Barring while roaming / WLAN

G.15.16.1 Definition

Test to verify that the UE activates and deactivates the "IMS Multimedia Telephony Communication Barring for outgoing calls while the user is roaming" supplementary service while camping on HPLMN. This process is described in 3GPP TS 24.611 [101].

G.15.16.2 Conformance requirement

As described in clause 15.14b.2.

G.15.16.3 Test purpose

As described in clause 15.14b.3.

G.15.16.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Outgoing Communication Barring, at step 7 deactivation of Outgoing Communication Barring is respectively triggered at the UE.

G.15.16.5 Test requirements

As described in clause 15.14b.5

G.15.17 Subscription to the MWI event package / WLAN

G.15.17.1 Definition

Test to verify that the UE is able to subscribe to MTSI message waiting notification and handle such notifications received after subscription. This process is described in 3GPP TS 24.229 [10] and TS 24.606 [107].

G.15.17.2 Conformance requirement

As described in clause 15.15.2.

G.15.17.3 Test purpose

As described in clause 15.15.3.

G.15.17.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS according the procedure C.2c steps 1-5.

The UE is pre-configured to autonomously subscribe to the Message Waiting Indication package. The UE is configured with the public service identity of the message account. Otherwise the phone is expected to use the public identity of the user when subscribing to the Message Waiting Indication package.

Test procedure

As described in clause 15.15.4.

G.15.17.5 Test requirements

As described in clause 15.15.5.

G.15.18 Inviting user to conference by sending a REFER request to the conference focus / WLAN

G.15.18.1 Definition

Test to verify that the UE is able to invite a user to a conference by sending a REFER request to the conference focus. This process is described in 3GPP TS 24.147 [84].

G.15.18.2 Conformance requirement

As described in clause 15.19.2.

G.15.18.3 Test purpose

As described in clause 15.19.3.

G.15.18.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and created a conference according the procedure C.2c and C.10a.

Test procedure

As described in clause 15.19.4.

G.15.18.5 Test requirements

As described in clause 15.19.5.

G.15.19 Joining a conference after being invited to it / WLAN

G.15.19.1 Definition

Test to verify that the UE is able to join a MTSI voice conference after being invited to it. This process is described in 3GPP TS 24.147 [84].

G.15.19.2 Conformance requirement

As described in clause 15.21.2.

G.15.19.3 Test purpose

As described in clause 15.21.3.

G.15.19.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MT call according the procedures C.2c and C.11a.

Test procedure

As described in clause 15.21.4.

G.15.19.5 Test requirements

As described in clause 15.21.5.

G.15.20 Three way session creation / WLAN

G.15.20.1 Definition

Test to verify that the UE support Three Way Session creation. This process is described in Section 5.3.1.3.3 of 3GPP TS 24.147 [84].

G.15.20.2 Conformance requirement

As described in clause 15.21a.2.

G.15.20.3 Test purpose

As described in clause 15.21a.3.

G.15.20.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MO call according the procedures C.2c and C.21a.

Test procedure

As described in clause 15.21a.4, but, steps 5-17 replaced by steps 1-8 in C.21a, steps 19-30 are replaced by steps 2-9 in C.10a.

G.15.20.5 Test requirements

As described in clause 15.21a.5.

G.15.21 Inviting user to conference by sending a REFER request to the conference focus for video / WLAN

G.15.21.1 Definition

Test to verify that the UE is able to invite a user to a conference by sending a REFER request to the conference focus. This process is described in 3GPP TS 24.147 [84].

G.15.21.2 Conformance requirement

As described in clause 15.19a.2.

G.15.21.3 Test purpose

As described in clause 15.19a.3.

G.15.21.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and created a conference according the procedure C.2c and C.38a.

Test procedure

As described in clause 15.19a.4.

G.15.21.5 Test requirements

As described in clause 15.19a.5.

G.15.22 Joining a conference after being invited to it with video / WLAN

G.15.22.1 Definition

Test to verify that the UE is able to join a MTSI video conference after being invited to it. This process is described in 3GPP TS 24.147 [84].

G.15.22.2 Conformance requirement

As described in clause 15.21b.2.

G.15.22.3 Test purpose

As described in clause 15.21b.3.

G.15.22.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MT video call according the procedures C.2c and C.26a.

Test procedure

As described in clause 15.21b.4.

G.15.22.5 Test requirements

As described in clause 15.21b.4.

G.15.23 Three way session creation for video / WLAN

G.15.23.1 Definition

Test to verify that the UE support Three Way Session creation for Video. This process is described in Section 5.3.1.3.3 of 3GPP TS 24.147 [84].

G.15.23.2 Conformance requirement

As described in clause 15.21c.2.

G.15.23.3 Test purpose

As described in clause 15.21c.3.

G.15.23.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MO video call according the procedures C.2c and C.25a.

Test procedure

As described in clause 15.21c.4, except, steps 5-17 replaced by steps 1-8 in C.25a, steps 19-26 replaced by steps C.10a.

G.15.23.5 Test requirements

As described in clause 15.21c.5.

G.15.24 Communication Waiting and answering the call / WLAN

G.15.24.1 Definition

Test to verify that the MT UE correctly performs MTSI Communication Waiting. This process is described in 3GPP TS 24.615 [95].

G.15.24.2 Conformance requirement

As described in clause 15.27.2.

G.15.24.3 Test purpose

As described in clause 15.27.3.

G.15.24.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MO call according the procedures C.2c and C.21a.

Test procedure

As described in clause 15.27.4, steps 1-15. Except, steps 1-8 replaced by steps 1-2C in C.11a.

G.15.24.5 Test requirements

As described in clause 15.27.5.

G.15.25 Communication Waiting and cancelling the call / WLAN

G.15.25.1 Definition

Test to verify that the UE correctly performs IMS Multimedia Telephony Communication Waiting (CW) terminal based procedure. This process is described in 3GPP TS 24.615 [95].

G.15.25.2 Conformance requirement

As described in clause 15.28.2.

G.15.25.3 Test purpose

As described in clause 15.28.3.

G.15.25.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS and set up the MO call according the procedures C.2c and C.21a.

Test procedure

As described in clause 15.28.4, steps 1-15. Except, steps 1-8 replaced by steps 1-2C in C.11a.

G.15.25.5 Test requirements

As described in clause 15.28.5.

G.16

G.17 Media use cases / WLAN

G.17.1 MO Speech, add video remove video / WLAN

G.17.1.1 Definition

Test to verify that the UE is able to correctly add a bidirectional video component to an ongoing mobile originated IMS Multimedia telephony voice call, and test to verify that the UE is able to correctly remove the bidirectional video component from the ongoing mobile originated IMS Multimedia video call, using WLAN access.

This process is described in 3GPP TS 24.229 [10], TS 24.173 [65] and TS 26.114 [66].

G.17.1.2 Conformance requirement

As described in clause 17.1.2.

G.17.1.3 Test purpose

As described in clause 17.1.3

G.17.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN). The UE has registered to IMS according the procedures C.2c and set up an MO call over WLAN by executing annex C.21a.

Test procedure

1) Adding video to the voice call is initiated on the UE.

2) UE sends a re-INVITE request to the SS.

3) SS responds to the re-INVITE request with a 100 Trying response.

4) SS responds to the re-INVITE request with valid 200 OK response.

5) UE acknowledges receipt of 200 OK for re-INVITE.

6) Removing video from the media call is initiated on the UE.

7) UE sends a re-INVITE request to the SS.

8) SS responds to the re-INVITE request with a 100 Trying response.

9) SS responds to the re-INVITE request with valid 200 OK response.

10) UE acknowledges receipt of 200 OK for re-INVITE.

11-12) MO Call release.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE add IMS video to voice call	
2	→		INVITE	UE sends re-INVITE with an SDP offer containing media lines for both voice and video.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		200 OK	SS sends a 200 OK for INVITE.
5	→		ACK	UE acknowledges the receipt of 200 OK for re-INVITE.
6			Make UE release video from media call	
7	→		INVITE	UE sends re-INVITE with an SDP offer indicating that the video component is removed from the call
8	←		100 Trying	SS sends a 100 Trying provisional response.
9	←		200 OK	The SS responds re-INVITE with 200 OK
10	→		ACK	The UE acknowledges the receipt of 200 OK for re-INVITE
11	→		BYE	UE releases the call
12	←		200 OK	SS sends 200 OK for BYE

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 4] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 3] - *a=pcfg:1 t=1* [Note 3] - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id*= (att-field) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be "/1" or omitted. Note 3: The tcap/pcfg attributes are present if RTP/AVP is present on the m line. Note 4: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

200 OK (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 2] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=acfg:1 t=1* [Note 3] - *a=rtpmap:* (payload type) *H264/90000* [Note 1] - *a=fmtp:* (format) (format specific parameters) [Note 1] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: The value for fmt, bandwidth, payload type, format and format specific parameters copied from step 2. Note 2: Transport port is the port number of the SS (see RFC 3264 clause 6). Note 3: Present if tcap/pcfg attributes were included in step 2.

INVITE (Step 7)

Use the default message “INVITE for MO Call” in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3] - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Media description: - *m=video 0 RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one. Note 3: The AMR channel number shall be “/1” or omitted.

200 OK (Step 9)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length Value	 length of message-body
Message-body	SDP body of the 200 response copied from the received INVITE and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and, for audio, transport port on "m=" line changed to indicate to which IP address and port the UE should start sending the media;

G.17.1.5 Test requirements

As described in clause 17.1.5

G.17.2 MT Speech, add video remove video / WLAN

G.17.2.1 Definition

Test to verify that the UE is able to correctly add a bidirectional video component to an ongoing mobile terminated IMS Multimedia telephony voice call, and test to verify that the UE is able to correctly remove the bidirectional video component from the ongoing mobile terminated IMS Multimedia video call, using WLAN access.

This process is described in 3GPP TS 24.229 [10], TS 24.173 [65] and TS 26.114 [66].

G.17.2.2 Conformance requirement

As described in clause 17.2.2.

G.17.2.3 Test purpose

As described in clause 17.2.3

G.17.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN). The UE has registered to IMS according the procedures C.2c and SS set up an MT call over WLAN by executing annex C.11a.

Test procedure

1) SS sends a re-INVITE request to the UE in order to add video to the ongoing call.

2) UE optionally responds to the re-INVITE request with a 100 Trying response.

2A) SS may receive 183 Session Progress from the UE.

2B) SS send PRACK to the UE to acknowledge the 183 Session Progress.

2C) SS receive 200 OK for PRACK from the UE.

2D) The UE accepts the session modification.

3) SS expects and receives 200 OK for re-INVITE from the UE.

4) SS acknowledges receipt of 200 OK for re-INVITE.

5) SS sends a re-INVITE request to the SS in order to remove video from the ongoing call.

6) UE optionally responds to the re-INVITE request with a 100 Trying response.

7) UE responds to the re-INVITE request with valid 200 OK response.

8) SS acknowledges receipt of 200 OK for re-INVITE.

9-10) MT Call release.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends re-INVITE with an SDP offer containing media lines for both voice and video.
2	→		100 Trying	(Optional) UE sends a 100 Trying provisional response.
2A	→		183 Session Progress	(Optional) The UE sends 183 response reliably with the SDP answer to the offer in INVITE
2B	←		PRACK	(Optional) SS acknowledges the receipt of 183 response from the UE.
2C	→		200 OK	(Optional) The UE responds to PRACK with 200 OK
2D				Make UE accept the speech and video offer.
3	→		200 OK	The UE responds to re-INVITE with 200 OK and includes SDP answer if SDP answer was not included with 183 Session Progress in step 2A.
4	←		ACK	SS acknowledges the receipt of 200 OK for re-INVITE.
5	←		INVITE	UE sends re-INVITE with an SDP offer indicating that the video component is removed from the call
6	→		100 Trying	SS sends a 100 Trying provisional response.
7	→		200 OK	The SS responds re-INVITE with 200 OK
8	←		ACK	The UE acknowledges the receipt of 200 OK for re-INVITE
9	←		BYE	SS send BYE
10	→		200 OK	UE sends 200 OK for BYE

Specific Message Content

INVITE (Step 1)

Use the default message "INVITE for MO Call" in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - *s=-* - *c= IN* (addrtype) (connection-address for SS) - *b=AS:352* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap: 97 AMR-WB/16000/1* - *a=fmtp: 97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF 101* - *b=AS:315* - *b=RS:0* - *b=RR:2500* Attributes for media: - *a=rtpmap:1018 H264/90000* - *a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; \ sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=rtcp-fb:* trr-int 5000* - *a=rtcp-fb:* nack* - *a=rtcp-fb:* nack pli* - *a=rtcp-fb:* ccm fir* - *a=rtcp-fb:* ccm tmmbr* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 2A)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) [Note 3] - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: *- a=curr:qos local sendrecv* *- a=curr:qos remote sendrecv* *- a=des:qos mandatory local sendrecv* *- a=des:qos mandatory remote sendrecv* Media description: - *m=video* (transport port) *RTP/AVPF (fmt)* - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (payload type) *packetization-mode=0;profile-level-id= (att-field); * Attributes for preconditions: *- a=curr:qos local sendrecv* *- a=curr:qos remote sendrecv* *- a=des:qos mandatory local sendrecv* *- a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be “/1” or omitted. Note 3: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one

200 OK (Step 3)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/Remark
Require option-tag	 *precondition*
Message-body	Present if there has been no SDP answer at step 2A. Contents if present: Same as specified in step 2A.

INVITE (Step 5)

Use the default message "INVITE for MO Call" in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS: 37* - *b=RS: 0* - *b=RR: 2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video 0 RTP/AVPF 101* - *b=AS: 315* - *b=RS: 0* - *b=RR: 2500* Attributes for media: - *a=rtpmap: 101 H264/90000* - *a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; \ sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

200 OK (Step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	SDP body not checked.

G.17.2.5 Test requirement

As described in clause 17.2.5

G.18

G.19 Emergency Service over IMS

G.19.1 Emergency call with emergency registration / WLAN

G.19.1.1 Definition

Test to verify that the UE can correctly register to IMS emergency services and initiate an IMS emergency call over WLAN when UE is registered to IMS non-emergency services of the HPLMN either with ISIM or USIM.

G.19.1.2 Conformance requirement

[TS 24.229 Rel-14, annex R.2.2.6]:

In this release of the specification, a WLAN, conforming to the requirements in this annex, defines emergency bearers. Emergency session is supported over the WLAN access if the UE has failed or has not been able to use 3GPP access to set up an emergency session as described in 3GPP TS 23.167 [4B] Annex J.

…

EPC procedures for emergency session using WLAN are defined for both trusted WLAN access via S2a, depending on the TWAN usage mode, anduntrusted WLAN access via S2b to access EPC.

When the IM CN subsystem is selected as the domain for the emergency call attempt, and the UE uses:

- untrusted WLAN access via S2b, the UE determines that the EPC supports emergency bearer services by selecting or using an ePDG that has indicated its capability of support for emergency services, as specified in subclause 7.2.1A of 3GPP TS 24.302 [8U];

…

Once IPsec tunnel setup is completed, the UE shall follow the procedures described in subclause R.2.2.1 of this specification for establishment of IP-CAN bearer and P-CSCF discovery accordingly.

…

When the emergency session ends, the UE:

1) shall release the tunnel as described in 3GPP TS 24.302 [8U]; and

2) if EPC via WLAN is the preferred IP-CAN to access IM CN subsystem or if no 3GPP access is available:

   a) if the UE did not select the currently selected ePDG using procedures for selection of ePDG for non-emergency services, shall select an ePDG for non-emergency services as described in 3GPP TS 24.302 [8U];

   b) if the UE does not have an IP-CAN bearer for non-emergency SIP signalling, shall follow the procedures described in subclause R.2.2.1 for establishment of an IP-CAN bearer for SIP signalling and P-CSCF discovery; and

   c) if the UE determines that its contact associated with the IP-CAN bearer for non-emergency SIP signalling is not bound to a public user identity, shall perform an initial registration as specified in subclause 5.1.1.2 using the IP-CAN bearer for SIP signalling.

[TS 24.302 Rel-14, clause 7.2.1A]:

The UE performs ePDG selection for emergency bearer services based on the ePDG configuration information provided by the home operator in the UE via H-ANDSF or via USIM, or via implementation specific means:

The ePDG configuration information used for selecting the ePDG for emergency bearer services includes:

- when available in ANDSF MO, Emergency_ePDG_Identifier and ePDG selection information are provisioned in ePDG node under Home Network Preference as specified in 3GPP TS 24.312 [13]; and

- when available in the USIM, the Emergency ePDG Identifier and ePDG selection information are provisioned in $EF_{ePDGIdEm}$ and $EF_{ePDGSelection}$ files as specified in 3GPP TS 31.102 [45].

NOTE: Implementation specific means apply only if the configurations via H-ANDSF and USIM are not present.

When performing ePDG selection for establishing emergency bearer services, the UE shall proceed by following the general ePDG selection procedure specified in subclause 7.2.1 except:

- Emergency_ePDG_Identifier shall be used instead of Home ePDG identifier;

- All ePDG FQDNs and visited country FQDNs for DNS query shall be constructed based on the ePDG FQDN format defined for emergency services as defined in 3GPP TS 23.003 [3]; and

- If the ME is not equipped with a UICC, the UE shall consider the ePDG configuration information as not available.

[TS 24.302 Rel-14, clause 7.2.5]:

If the UE needs to establish an IMS emergency session over untrusted non-3GPP access as specified in 3GPP TS 24.229 [67], the UE shall:

- if the UE is not connected to an ePDG yet, select an ePDG that supports emergency services as described in subclause 7.2.1A;

…

Once the UE selects an ePDG that supports emergency services as specified in subclause 7.2.1A, the UE shall initiate an IKEv2 tunnel establishment procedure towards this new ePDG as described in subclause 7.2.2.

G.19.1.3 Test purpose

1) To verify that the UE sends a correctly composed initial SIP REGISTER request for emergency services to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.6.1; and

2) To verify that the UE is able to use the IMS security procedures for the IMS emergency registration, as defined for IMS AKA and IPSec within 3GPP TS 24.229 [10] clause 5.1.1; and

3) To verify that the UE sends a correctly composed SIP INVITE request for the emergency call setup and will correctly complete the emergency session setup according to 3GPP TS 24.229 [10] clauses 5.1.6.8.3 and 6.1.2; and

4) To verify that at IMS emergency call release, the UE performs an initial IMS registration.

G.19.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS over WLAN according to procedure C.2c.

Test procedure

0) UE executes the procedure described in TS 36.508 [94] Table 4.5A.24.3-1.

1-4) UE performs IMS emergency registration and IMS emergency speech call.

10-12) Call is released on the UE.

12A) The UE initiates a disconnection from the IPsec tunnel set up for the emergency session as defined in 36.508 [94] Table 4.5A.23A.3-1.

Expected sequence:

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-4			Steps defined in clause C.20	IMS emergency registration by the UE
5-9			Steps defined in clause C.22	IMS emergency call setup with PSAP
10-12			Steps 1-3 defined in clause C.32	The UE releases the call
12A				IPsec tunnel disconnection procedure according to TS 36.508 [94] subclause 4.5A.23A.3

Specific Message Contents

INVITE (Step 5)

Use the default message “INVITE for MO call setup” in annex A.2.1 with condition A7 (INVITE for creating an emergency session within an emergency registration).

180 Ringing (Step 7)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with condition A4 (180 sent by the SS when setting up an emergency call).

200 OK (Step 8)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with condition A6 (Response sent by SS for INVITE for emergency call).

G.19.1.5 Test requirements

The UE shall send requests and responses as described in clause G.19.1.4.

Annex H (normative): IP-Connectivity Access Network specific test cases when using xDSL, Fiber or Ethernet to access IM CN subsystem

H.1 Scope

The present annex defines IP-CAN specific test cases for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is xDSL, Fiber or Ethernet.

NOTE: Fixed-broadband access in this Annex refers to xDSL, Fiber and Ethernet accesses.

H.2 to H.7

H.8 Registration

H.8.1 Initial registration / Fixed Broadband Access

H.8.1.1 Definition

Test to verify that the UE can correctly register to IMS services. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing the registration event package for the registered default public user identity.

H.8.1.2 Conformance requirement

[TS 24.229, 5.1.1.1B.1]:

In case the UE contains neither an ISIM nor a USIM, but IMC is present the UE shall use preconfigured parameters in the IMC to initiate the registration to the IM CN subsystem and for authentication.

The following IMS parameters are assumed to be available to the UE:

- a private user identity;
- a public user identity; and
- a home network domain name to address the SIP REGISTER request to.

These parameters may not necessarily reside in a UICC.

The first public user identity in the list stored in the IMC is used in emergency registration requests.

[TS 24.229 Rel-12, clause 5.1.1.2.1]:

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

When registering any public user identity belonging to the UE, the UE shall either use an already active pair of security associations or a TLS session to protect the REGISTER requests, or register the public user identity via a new initial registration procedure.

When binding any one of its public user identities to an additional contact address via a new initial registration procedure, the UE shall follow the procedures described in RFC 5626 [92]. The set of security associations or a TLS session resulting from this initial registration procedure will have no impact on the existing set of security associations or TLS sessions that have been established as a result of previous initial registration procedures. However, if the UE registers any one of its public user identities with a new contact address via a new initial registration procedure and does not employ the procedures described in RFC 5626 [92], then the new set of security associations or TLS session shall replace any existing set of security association or TLS session.

If the UE detects that the existing security associations or TLS sessions associated with a given contact address are no longer active (e.g., after receiving no response to several protected messages), the UE shall:

- consider all previously registered public user identities bound to this security associations or TLS session that are only associated with this contact address as deregistered; and
- stop processing all associated ongoing dialogs and transactions that were using the security associations or TLS session associated with this contact address, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs).

The UE shall send the unprotected REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, or if the UE was pre-configured with the P-CSCF's IP address or domain name and was unable to obtain specific port information, the UE shall send the unprotected REGISTER request to the SIP default port values as specified in RFC 3261 [26].

NOTE 1: The UE will only send further registration and subsequent SIP messages towards the same port of the P-CSCF for security mechanisms that do not require using negotiated ports for exchanging protected messages.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains:
   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else
   2) the public user identity to be registered;
b) a To header field set to the SIP URI that contains:
   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else
   2) the public user identity to be registered;
c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE:
   1) supports GRUU (see table A.4, item A.4/53);
   2) supports multiple registrations;
   3) has an IMEI available; or
   4) has an MEID available;

   the UE shall include a "+sip.instance" header field parameter containing the instance ID. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62].

if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Contact URI without a user portion and containing the "bnc" URI parameter;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. For the UDP, the UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223 [143];

NOTE 3: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 4: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and

k) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

a) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, the UE may initiate that mechanism on a media level when it initiates new media in an existing session.

NOTE 6: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header field value and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

NOTE 7: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the To header field will contain the main URI of the UE.

b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 8: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;

d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 9: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 10: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions (other than REGISTER method) when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:

- if the UE did not use the procedures specified in RFC 6140 [191] for registration, find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered; and

- if the UE used the procedures specified in RFC 6140 [191] for registration then find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter then store the value of the "pub-gruu" header field parameter for use for generating public GRUUs for registering UAs as specified in RFC 6140 [191]. If this contains a "temp-gruu-cookie" header field parameter then store the value of the "temp-gruu-cookie" header field parameter for use for generating temporary GRUUs for registering UAs as specified in RFC 6140 [191];

NOTE 11: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquely identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in subclause 7.1.2.2 of RFC 6140 [191].

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626 [92], and the S-CSCF has followed the registration procedure as described in RFC 5627 [93] or RFC 3261 [26], i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626 [92], the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626 [92]; or

NOTE 12: Upon replaces the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about the deregistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626 [92];

g) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session;

NOTE 13: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223 [143];

i) if the 200 (OK) response includes a Feature-Caps header field, as specified in RFC 6809°[190], with "+g.3gpp.icsi-ref" header field parameter, then the UE may consider the values included in the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field of 200 (OK) response as supported by the IM subsystem for the established registration or registration flow (if the multiple registration mechanism is used); and

NOTE 14: The UE and related applications can use the ICSI values received in the Feature-Caps header field of 200 (OK) response to improve the user experience.

j) if the 200 (OK) response includes one or more Feature-Caps header fields containing the capability indicators listed in subclause 7.9A.7 that indicate the media capabilities supported by the IMS-AGW then the UE may consider this information when providing media options to the user or determining whether an application communication capability will be successful (e.g. if "sip.video" is not indicated then the UE might not offer the user the option to attempt to add video to the session).

NOTE 15: If media capability indication is not supported, no capability indicators listed in subclause 7.9A.7 are included and it can be assumed that all the media capabilities are supported.

On receiving a 305 (Use Proxy) response to the unprotected REGISTER request, unless otherwise specified in access specific annexes (as described in Annex B or Annex L), the UE shall:

a) ignore the contents of the Contact header field if it is included in the received message;

NOTE 16: The 305 response is not expected to contain a Contact header field.

b) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

c) initiate either a new P-CSCF discovery procedure as described in subclause 9.2.1, or select a new P-CSCF, if the UE was pre-configured with more than one P-CSCF's IP addresses or domain names;

d) select a P-CSCF address, which is different from the previously used address, from the address list; and

e) perform the procedures for initial registration as described in subclause 5.1.1.2.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) or 600 (Busy Everywhere) response for an initial registration, the UE may attempt to perform initial registration again.

When the timer F expires at the UE, the UE may:

a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1 or from its pre-configured list of P-CSCF's IP addresses or domain names;

b) if no response has been received when attempting to contact all P-CSCFs known by the UE, get a new set of P-CSCF-addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in Annex B or Annex L); and

c) perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 17: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

On receiving a 4xx, 5xx or 6xx response to the REGISTER request, whereby the response contains a Retry-After header field, the UE shall not automatically attempt an initial registration via the same IP-CAN and the same P-CSCF for the amount of time indicated in the Retry-After header field. If the UE is power cycled, the UE can attempt an initial registration. If no initial registration occurs within the time period indicated by the Retry-After header field, the counter of unsuccessful initial registration attempts is reset.

After a first unsuccessful initial registration attempt, if the Retry-After header field was not present and the initial registration was not performed as a consequence of a failed reregistration, the UE shall not wait more than 5 minutes before attempting a new registration.

After a maximum of 2 consecutive unsuccessful initial registration attempts, if the Retry-After header field was not present in failure responses of those unsuccessful initial registration attempts, the UE shall implement the mechanism defined in subclause 4.5 of RFC 5626 [92] for new registration attempts. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in subclause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time have been provided to the UE by the network, the default values defined in subclause 4.5 of RFC 5626 [92] shall be used.

The values of max-time and base-time may be provided by the network to the UE using OMA-DM with the management objects specified in 3GPP TS 24.167 [8G]. Other mechanisms may be used as well and are outside the scope of the present specification.

[TS 24.229, clause 5.1.1.2.3]:

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 [21] unless otherwise specified in the access specific annexes, with:

- the "username" header field parameter, set to the value of the private user identity;
- the "realm" header field parameter, set to the domain name of the home network;
- the "uri" header field directive, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to an empty value; and
- the "response" header field parameter, set to an empty value;

b) the hostport parameter in the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent requests; and

c) the sent-by field in the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

The UE shall use the locally available public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration. The method whereby the public user identity and private user identity are made available to the UE is outside the scope of this document (e.g. a public user identity could be input by the end user).

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.4.

[TS 24.229, clause 5.1.1.5.4]:

On receiving a 401 (Unauthorized) response to the REGISTER request, and where the "algorithm" Authorization header field parameter is "MD5", the UE shall:

1) extract the digest-challenge parameters as indicated in RFC 2617 [21] from the WWW-Authenticate header field;

2) store the contained nonce value as the nonce for authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and delete any other previously stored nonce value for authentication for this registration or registration flow (if the multiple registration mechanism is used);

NOTE: The related registration flow or registration is identified by the couple instance-id and reg-id if the multiple registration mechanism is used or by contact address if not.

3) calculate digest-response parameters as indicated in RFC 2617 [21];

4) send another REGISTER request containing an Authorization header field. The header fields are populated as defined in subclause 5.1.1.2.3, with the addition that the UE shall include an Authorization header field containing a challenge response, constructed using the stored nonce value for authentication for the same registration or registration flow (if the multiple registration mechanism is used) "cnonce", "qop", and "nonce-count" header field parameters as indicated in RFC 2617 [21]. The UE shall set the Call-ID of the REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge. If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header fields with this REGISTER.

On receiving the 200 (OK) response for the REGISTER request, if the "algorithm" Authentication-Info header field parameter is "MD5", the UE shall authenticate the S-CSCF using the "rspauth" Authentication-Info header field parameter as described in RFC 2617 [21]. If the nextnonce field is present in the Authentication-Info header field the UE shall store the contained nonce value as the nonce for authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for authentication for this registration or registration flow (if the multiple registration mechanism is used).

[TS 24.229 Rel-12, clause 5.1.1.3]:

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680 [43] and RFC 6665 [28].

NOTE 1: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the subscription will be directed to the main URI, as described in RFC 6140 [191].

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package.

NOTE 2: The subscription information stored in the HSS ensures that the default public user identity is a SIP URI.

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to the SIP URI that is the default public user identity used for subscription;

b) a From header field set to the SIP URI that is the default public user identity used for subscription;

c) a To header field set to the SIP URI that is the default public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) void; and

g) void.

Upon receipt of a dialog establishing NOTIFY request, as specified in RFC 6665 [28], associated with the SUBSCRIBE request, the UE shall:

1) store the information for the established dialog;

2) store the expiration time as indicated in the "expires" header field parameter of the Subscription-State header field, if present, of the NOTIFY request. Otherwise the expiration time is retrieved from the Expires header field of the 2xx response to SUBSCRIBE request; and

3) follow the procedures specified in RFC 6665 [28].

If continued subscription is required, the UE shall automatically refresh the subscription by the reg event package, for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less. If a SUBSCRIBE request to refresh a subscription fails with a non-481 response, the UE shall still consider the original subscription valid for the duration of the most recently known "Expires" value according to RFC 6665 [28]. Otherwise, the UE shall consider the subscription invalid and start a new initial subscription according to RFC 6665 [28].

[TS 24.229, clause 5.1.2.1]:

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID header field, and the values of tags in To and From header fields).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package the UE shall perform the following actions:

- if a state attribute "active", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;

- if a state attribute "active" is received, and the UE supports GRUU (see table A.4, item A.4/53), then for each public user identity indicated in the notification that contains a <pub-gruu> element or a <temp-gruu> element or both (as defined in RFC 5628) then the UE shall store the value of those elements in association with the public user identity;

- if a state attribute "terminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered and shall remove any associated GRUUs.

NOTE 1: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity or when S-CSCF receives a Push-Profile-Request (PPR) from the HSS (as described in 3GPP TS 29.228) changing the status of a public user identity associated with a registered implicit set from barred to non-barred. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE. The implicitly registered public user identities may also belong to different service profiles. The here-described procedures provide a different mechanism (to the 200 (OK) response to the REGISTER request) to inform the UE about these automatically registered public user identities.

NOTE 2: RFC 5628 provides guidance on the management of temporary GRUUs, utilizing information provided in the reg event notification.

[TS 24.229, clause 5.1.2A.1.1]:

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using either a given contact address, or to the registration flow and the associated contact address the UE shall:

- if IMS AKA is in use as a security mechanism:

    a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

    b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

- if SIP digest without TLS is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the port value of an unprotected port and the contact address where the UE expects to receive subsequent mid-dialog requests; and

  b) populate the Via header field of the request with the port value of an unprotected port and the respective contact address where the UE expects to receive responses to the request;

...

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

NOTE 13: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs and standalone transactions. The UE shall build a list of Route header field values made out of the following, in this order:

a) the P-CSCF URI containing the IP address or the FQDN learnt through the P-CSCF discovery procedures; and

b) the P-CSCF port based on the security mechanism in use:

   - if IMS AKA or SIP digest with TLS is in use as a security mechanism, the protected server port learnt during the registration procedure;

   - if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is in use as a security mechanism, the unprotected server port used during the registration procedure;

c) and the values received in the Service-Route header field saved from the 200 (OK) response to the last registration or re-registration of the public user identity with associated contact address.

[TS 24.229, clause E.3.1.0]:

In order to reach IMS in some access networks, the UE may support:

- address and/or port number conversions provided by a NA(P)T or NA(P)T-PT as described in annex F and annex K; and

- UE requested FTT-IMS establishment procedure specified in 3GPP TS 24.322 [8Y].

If a UE supports one or both of these capabilities then a UE may progressively try them to overcome failure to reach the IMS. Use of these capabilities shall have the following priority order:

1) UE uses neither capability because reaching the IMS without an intervening NA(P)T, NA(P)T-PT, or tunnel is preferred.

2) UE may use address and/or port number conversions provided by a NA(P)T or NA(P)T-PT as described in either annex F or annex K.

3) UE may use the UE requested FTT-IMS establishment procedure specified in 3GPP TS 24.322 [8Y]. If the UE uses the UE-requested FTT-IMS establishment procedure specified in 3GPP TS 24.322 [8Y], the UE considers itself to:

   - be configured to send keep-alives;

   - be directly connected to an IP-CAN for which usage of NAT is defined; and

   - be behind a NAT.

Optional procedures apply when the UE is supporting traversal of restrictive non-3GPP access network using STUN/TURN/ICE, as follows:

a) the protection of SIP messages is provided by utilizing TLS as defined in 3GPP TS 33.203 [19];

b) the mechanisms specified in this annex shall only be applicable when the IP traffic to the IMS core does not traverse through the Evolved Packet Core (EPC);

c) the UE shall establish the TLS connection to the P-CSCF on port 443. The UE shall use SIP digest with TLS for registration as specified in subclause 5.1. If the TLS connection is established successfully, the UE sends SIP signalling over the TLS connection to the P-CSCF;

d) the UE shall support the keep-alive procedures described in RFC 6223 [143];

NOTE 1: If the UE is configured to use an HTTP proxy, the UE use the HTTP CONNECT method specified in RFC 2817 [220] to request the HTTP proxy to establish the TCP connection with the P-CSCF. Once the UE has received a positive reply from the proxy that the TCP connection has been established, the UE initiates the TLS handshake with the P-CSCF and establishes the TLS connection.

e) the procedures described in subclause K.5.2 apply with the additional procedures described in the present subclause;

f) when using the ICE procedures for traversal of restrictive non-3GPP access network, the UE shall support the ICE TCP as specified in RFC 6544 [131] and TURN TCP as specified in RFC 6062 [221].

g) if the UE is configured to use TURN over TCP on port 80, the UE shall establish the TCP connection to TURN server on port 80. If the UE is configured to use TURN over TLS on port 443, the UE shall establish the TLS connection to the TURN server on port 443. If the UE is configured to use both, the UE should prefer to use TURN over TCP on port 80 to avoid TLS overhead;

h) if the connection is established successfully, the UE sends TURN control messages and media packets over the connection as defined in RFC 5766 [101].

NOTE 2: If the UE is configured to use an HTTP proxy, the UE use the HTTP CONNECT method specified in RFC 2817 [220] to request the HTTP proxy to establish the TCP connection with the TURN server. Then, if the UE is configured to use TURN over TLS on port 443 and the UE has received a positive reply from the proxy that the TCP connection has been established, the UE initiates the TLS handshake with the TURN server and establishes the TLS connection.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.1B.1, 5.1.1.2.1, 5.1.1.2.3, 5.1.1.5.4, 5.1.1.3, 5.1.2.1, 5.1.2A.1.1 and E.3.1.0.

H.8.1.3 Test purpose

1) To verify that the UE sends a correctly composed initial REGISTER request to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.1.3;

2) To verify that after receiving a valid 401 (Unauthorized) response from S-CSCF for the initial REGISTER sent, the UE correctly authenticates itself by sending another REGISTER request with correctly composed Authorization header using MD5 algorithm (as described in RFC 3310 [17]); and

3) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER sent for authentication, the UE stores the default public user identity and information about barred user identities; and

4) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER sent for authentication, the UE subscribes to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in RFC 3680 [22]; and

5) To verify that the UE uses the default public user identity for subscription to the registration-state event package, when the public user identity that was used for initial registration is a barred public user identity; and

6) To verify that the UE uses the stored service route for routing the SUBSCRIBE sent; and

7) To verify that after receiving a valid 200 OK response from S-CSCF to the SUBSCRIBE sent for registration event package, the UE maintains the generated dialog; and

8) To verify that after receiving a valid NOTIFY for the registration event package, the UE will update and store the registration state of the indicated public user identities accordingly (as specified in RFC 3680 [22] clause 5); and

9) To verify that the UE responds the received valid NOTIFY with 200 OK.

H.8.1.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1) IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request.

2) SS responds to the initial REGISTER request with a valid 401 Unauthorized response, headers populated according to the 401 response common message definition.

3) SS waits for the UE to another REGISTER request.

4) SS responds to the second REGISTER request with valid 200 OK response. SS shall populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

5) SS waits for the UE to send a SUBSCRIBE.

6) SS responds to the SUBSCRIBE request with a valid 200 OK response, headers populated according to the 200 response for SUBSCRIBE common message definition.

7) SS sends UE a NOTIFY request for the subscribed registration event package. In the request the Request URI, headers and the request body shall be populated according to the NOTIFY common message definition.

8) SS waits for the UE to respond the NOTIFY with 200 OK response.

Expected sequence

Step	Direction UE SS	Message	Comment
1	→	REGISTER	UE sends initial registration for IMS services.
2	←	401 Unauthorized	The SS responds with a valid MD5 authentication challenge
3	→	REGISTER	SS sends another REGISTER with MD5 valid credentials.
4	←	200 OK	The SS responds with 200 OK.
5	→	SUBSCRIBE	UE subscribes to its registration event package.
6	←	200 OK	The SS responds SUBSCRIBE with 200 OK
7	←	NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
8	→	200 OK	The UE responds the NOTIFY with 200 OK

Specific Message Contents

REGISTER (Step 1)

Use the default message “REGISTER” in annex A.1.1 with condition A14 "Initial REGISTER over Fixed Access Broadband"

401 Unauthorized for REGISTER (Step 2)

Use the default message “401 Unauthorized for REGISTER” in annex A.1.2 with condition A2 " SIP Digest without TLS for Fixed Broadband Access "

REGISTER (Step 3)

Use the default message “REGISTER” in annex A.1.1 with condition A15 "Subsequent REGISTER over Fixed Access Broadband”

200 OK for REGISTER (Step 4)

Use the default message “200 OK for REGISTER” in annex A.1.3 with condition A5 " SIP Digest without TLS for Fixed Broadband Access "

SUBSCRIBE (Step 5)

Use the default message “SUBSCRIBE for reg-event package” in annex A.1.4 with condition A5 " SIP Digest without TLS for Fixed Broadband Access "

200 OK for SUBSCRIBE (Step 6)

Use the default message “200 OK for SUBSCRIBE” in annex A.1.5 with condition A3 " SIP Digest without TLS for Fixed Broadband Access "

NOTIFY (Step 7)

Use the default message “NOTIFY for reg-event package” in annex A.1.6 with condition A5 " SIP Digest without TLS for Fixed Broadband Access "

200 OK for NOTIFY (Step 8)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1

H.8.1.5 Test requirements

If the UE is preconfigured with the home domain name, public and private user identities and SIP Digest Credentials

Step 1: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.3 the UE sends a REGISTER.

Step 3: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5 the UE sends another REGISTER request.

Step 5: SS shall check that, in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.3, the UE sends a SUBSCRIBE request for registration event package.

H.8.2 User Initiated Re-Registration / Fixed Broadband Access

H.8.2.1 Definition

Test to verify that the UE can re-register a previously registered public user identity at any time. This process is described in 3GPP TS 24.229 [10], clause 5.1.1.4. The test case is applicable for IMS security.

H.8.2.2 Conformance requirement

[TS 24.229, clause 5.1.1.4.1]:

The UE can perform the reregistration of a previously registered public user identity bound to any one of its contact addresses and the associated set of security associations or TLS sessions at any time after the initial registration has been completed.

The UE can perform the reregistration of a previously registered public user identity over any existing set of security associations or TLS session that is associated with the related contact address.

The UE can perform the reregistration of a previously registered public user identity via an initial registration as specified in subclause 5.1.1.2, when binding the previously registered public user identity to new contact address.

The UE can perform registration of additional public user identities at any time after the initial registration has been completed. The UE shall perform the registration of additional public user identities either:

- over the existing set of security associations or TLS sessions, if appropriate to the security mechanism in use, that is associated with the related contact address; or
- via an initial registration as specified in subclause 5.1.1.2.

The UE can fetch bindings as defined in RFC 3261 at any time after the initial registration has been completed. The procedure for fetching bindings is the same as for a reregistration except that the REGISTER request does not contain a Contact header field.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister an already registered public user identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 or when the UE needs to modify the ICSI values that the UE intends to use in a g.3gpp.icsi-ref media feature tag or IARI values that the UE intends to use in the g.3gpp.iari-ref media feature tag.

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203, established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep;

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 2: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep, towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229, clause 5.1.1.4.3]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 [21], including:

- the "username" header field parameter, set to the value of the private user identity;
- the "realm" header field parameter, set to the domain name of the home network;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

- the "nonce" header field parameter, set to the stored nonce value for authentication for the related registration or registration flow (if the multiple registration mechanism is used); and

NOTE: The related registration flow or registration is identified by the couple instance-id and reg-id if the multiple registration mechanism is used or by contact address if not.

- the "response" header field parameter, set to the challenge response, constructed using the stored nonce value for authentication for the same registration or registration flow (if the multiple registration mechanism is used), along with "cnonce", "qop", and "nonce-count" header field parameters as specified in RFC 2617 [21];

b) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent requests; and

c) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.4.1 and 5.1.1.4.3.

H.8.2.3 Test purpose

1) To verify that the UE can re-register a previously registered public user identity at either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less; and

2) Extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration; and

3) To verify that the UE populates the header field in the REGISTER request with From, To, Via, Contact, Authorization, Expires, Supported, and P-Access-Network-Info headers; and

4) Upon receiving 200 OK for REGISTER, the UE shall store the new expiration time of the registration for this public user identity, the list of URIs contained in the P-Associated-URI header value and use these values in the next re-register request.

H.8.2.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1-8) The same procedure as in subclause H.8.1.4 are used with the exception that the SS sets the expiration time to 120 seconds in Step 4.

9) Before half of the time has expired from the initial registration SS receives re-register message request with the From, To, Via, Contact, Authorization, Expires, Supported, and P-Access-Network-Info header fields.

10) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1200 seconds) of the registration for this public user identity.

11) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

12) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1800 seconds) of the registration for this public user identity.

13) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

14) SS responds to the REGISTER request with valid 200 OK response. SS shall populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Messages in Initial Registration Test case (subclause H.8.1.4)	The same messages as in subclause H.8.1.4 are used with the exception that in Step 4, the SS responds with 200 OK indicating 120 seconds expiration time.
9	→		REGISTER	The SS receives REGISTER from the UE 60 seconds before the expiration time set in the initial registration request.
10	←		200 OK	The SS responds with 200 OK indicating 1200 seconds expiration time.
11	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 10.
12	←		200 OK	The SS responds with 200 OK indicating 1800 seconds expiration time.
13	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 12
14	←		200 OK	The SS responds with 200 OK indicating the default expiration time.

Specific Message Contents

Messages in Step 1-8

Messages in Step 1-8 are the same as those specified in subclause 8.1.4 with the following exception for the 200 OK for REGISTER in Step 4:

Use the default message “200 OK for REGISTER” in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	120

REGISTER (Step 9)

Use the default message “REGISTER” in annex A.1.1 with condition A15 "Subsequent REGISTER over Fixed Access Broadband”

200 OK for REGISTER (Step 10)

Use the default message “200 OK for REGISTER” in annex A.1.3 with condition A5 "SIP Digest without TLS for Fixed Broadband Access" and with the following exceptions:

Header/param	Value/remark
Contact	
expires	1200

REGISTER (Step 11)

Use the default message “REGISTER” in annex A.1.1 with condition A15 "Subsequent REGISTER over Fixed Access Broadband”

200 OK for REGISTER (Step 12)

Use the default message “200 OK for REGISTER” in annex A.1.3 with condition A5 "SIP Digest without TLS for Fixed Broadband Access"

REGISTER (Step 13)

Use the default message “REGISTER” in annex A.1.1 with condition A15 "Subsequent REGISTER over Fixed Access Broadband”

200 OK for REGISTER (Step 14)

Use the default message “200 OK for REGISTER” in annex A.1.3 with condition A5 "SIP Digest without TLS for Fixed Broadband Access"

H.8.2.5 Test requirements

1. The UE shall in step 9 send the REGISTER request within 60 seconds from the time instant that it receives 200 OK in step 4 from the SS.
2. The UE shall in step 11 send the REGISTER request within 600 seconds from the time instant that it receives 200 OK from the SS in step 10.
3. The UE shall in step 13 send the REGISTER request within 1200 seconds from the time instant that it receives 200 OK from the SS in step 12.

H.8.3 User Initiated Deregistration / Fixed Broadband Access

H.8.3.1 Definition

Test to verify that the UE can perform a correct de-registration procedure. This process is described in 3GPP TS 24.229 [10], clause 5.1.1.6.

H.8.3.2 Conformance requirement

[TS 24.229, clause 5.1.1.6.1]:

The UE can deregister a public user identity that it has previously registered with its contact address at any time. The UE shall protect the REGISTER request using a security association or TLS session that is associated with contact address, see 3GPP TS 33.203, established as a result of an earlier registration, if one is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs that were using the contact addresses that is going to be deregistered and related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities. However:

- if the dialog that was established by the UE subscribing to the reg event package used the public user identity that is going to be deregistered; and
- this dialog is the only remaining dialog used for subscription to reg event package of the user, i.e. there are no other contact addresses registered with associated subscription to the reg event package of the user;

then the UE shall not release this dialog.

On sending a REGISTER request that will remove the binding between the public user identity and one of its contact addresses, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be deregistered;

b) a To header field set to the SIP URI that contains the public user identity to be deregistered;

c) a Contact header field set to the SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, and containing the Instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE supports multiple registrations, it shall include "reg-id" header field parameter as described in RFC 5626;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field;

e) a registration expiration interval value set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

h) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

For a public user identity that the UE has registered with multiple contact addresses (e.g. via different P-CSCFs), the UE shall also be able to deregister multiple contact addresses, bound to its public user identity, via single deregistration procedure as specified in RFC 3261. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a list of Contact headers. Each Contact header in the list shall contain the contact addresses that the UE wants to deregister with the "expires" parameter containing the value equal zero.

The UE can deregister all contact addresses bound to its public user identity and associated with its private user identity. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a public user identity that is being deregistered in the To header field, and a single Contact header field with value of "*" and the Expires header field with a value of "0".

NOTE 2: All entities subscribed to the reg event package of the user will be inform via NOTIFY request which contact addresses bound to the public user identity have been deregistered.

When a 401 (Unauthorized) response to a REGISTER request is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- remove all registration details relating to this public user identity and the associated contact address.

- store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 9: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

If there are no more public user identities registered with this contact address, the UE shall delete any stored media plane security mechanisms and related keys and any security associations or TLS sessions and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and all security association or TLS session is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

[TS 24.229, clause 5.1.1.6.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter, set to the value of the private user identity;
- the "realm" header field parameter, set to the value as received in the "realm" WWW-Authenticate header field parameter;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to last received nonce value; and
- the response directive, set to the last calculated response value;

b) additionally for each Contact header field and associated contact address, include the associated protected server port value in the hostport parameter;

c) additionally for the Via header field, include the protected server port value bound to the security association in the sent-by field;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

d) a Security-Client header field, set to specify the signalling plane security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 and RFC 3329; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

NOTE 2: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with this contact address and its associated set of implicitly registered public user identities (i.e. no other public user identity is registered), the UE removes the security association (between the P-CSCF and the UE) that were using this contact address. Therefore further SIP signalling using this security association (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

[TS 24.229, clause E.3.1.0]:

In order to reach IMS in some access networks, the UE may support:

- address and/or port number conversions provided by a NA(P)T or NA(P)T-PT as described in annex F and annex K; and
- UE requested FTT-IMS establishment procedure specified in 3GPP TS 24.322 [8Y].

If a UE supports one or both of these capabilities then a UE may progressively try them to overcome failure to reach the IMS. Use of these capabilities shall have the following priority order:

1) UE uses neither capability because reaching the IMS without an intervening NA(P)T, NA(P)T-PT, or tunnel is preferred.

2) UE may use address and/or port number conversions provided by a NA(P)T or NA(P)T-PT as described in either annex F or annex K.

3) UE may use the UE requested FTT-IMS establishment procedure specified in 3GPP TS 24.322 [8Y]. If the UE uses the UE-requested FTT-IMS establishment procedure specified in 3GPP TS 24.322 [8Y], the UE considers itself to:

   - be configured to send keep-alives;

- be directly connected to an IP-CAN for which usage of NAT is defined; and
- be behind a NAT.

Optional procedures apply when the UE is supporting traversal of restrictive non-3GPP access network using STUN/TURN/ICE, as follows:

a) the protection of SIP messages is provided by utilizing TLS as defined in 3GPP TS 33.203 [19];

b) the mechanisms specified in this annex shall only be applicable when the IP traffic to the IMS core does not traverse through the Evolved Packet Core (EPC);

c) the UE shall establish the TLS connection to the P-CSCF on port 443. The UE shall use SIP digest with TLS for registration as specified in subclause 5.1. If the TLS connection is established successfully, the UE sends SIP signalling over the TLS connection to the P-CSCF;

d) the UE shall support the keep-alive procedures described in RFC 6223 [143];

NOTE 1: If the UE is configured to use an HTTP proxy, the UE use the HTTP CONNECT method specified in RFC 2817 [220] to request the HTTP proxy to establish the TCP connection with the P-CSCF. Once the UE has received a positive reply from the proxy that the TCP connection has been established, the UE initiates the TLS handshake with the P-CSCF and establishes the TLS connection.

e) the procedures described in subclause K.5.2 apply with the additional procedures described in the present subclause;

f) when using the ICE procedures for traversal of restrictive non-3GPP access network, the UE shall support the ICE TCP as specified in RFC 6544 [131] and TURN TCP as specified in RFC 6062 [221].

g) if the UE is configured to use TURN over TCP on port 80, the UE shall establish the TCP connection to TURN server on port 80. If the UE is configured to use TURN over TLS on port 443, the UE shall establish the TLS connection to the TURN server on port 443. If the UE is configured to use both, the UE should prefer to use TURN over TCP on port 80 to avoid TLS overhead;

h) if the connection is established successfully, the UE sends TURN control messages and media packets over the connection as defined in RFC 5766 [101].

NOTE 2: If the UE is configured to use an HTTP proxy, the UE use the HTTP CONNECT method specified in RFC 2817 [220] to request the HTTP proxy to establish the TCP connection with the TURN server. Then, if the UE is configured to use TURN over TLS on port 443 and the UE has received a positive reply from the proxy that the TCP connection has been established, the UE initiates the TLS handshake with the TURN server and establishes the TLS connection.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.6.1, 5.1.1.6.2 and E.3.1.0.

H.8.3.3 Test purpose

1) To verify that the UE sends a correctly composed initial REGISTER request with an expiration interval value set to 0 to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.1.6.

2) To verify that the UE sends correctly composed unsubscriptions, in case the UE unsubscribes from its event packages.

H.8.3.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

0) The UE is triggered by MMI to initiate a deregistration procedure.

0A-0D) UE optionally unsubscribes from event packages it had subscribed to.

1) IMS deregistration is initiated on the UE. SS waits the UE to send a REGISTER request, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.6.

2) SS responds to REGISTER with a correctly composed 200 OK message.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
0			Make the UE deregister from IMS	
0A-2			Steps 0A-2 defined in Annex C.30b	

H.8.3.5 Test Requirements

SS shall check in steps 0A-0D that the UE uses headers as described in C.30 in case it unsubscribes from event packages.

SS shall check in step 1 that the de-register request sent by the UE has the headers correctly populated as per the default message “REGISTER” in annex A.1.1condition A15.

H.8.4 Invalid behaviour- 423 Interval too brief / Fixed Broadband Access

H.8.4.1 Definition

As described in clause 8.4.1.

H.8.4.2 Conformance requirement

As described in clause 8.4.2.

H.8.4.3 Test purpose

As described in clause 8.4.3.

H.8.4.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1 IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request.

2 SS responds to the initial REGISTER request with a 423 (Interval Too Brief) response.

3 SS waits for the UE to send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

4 Continue test execution with the Generic test procedure in Annex C.2b, step 3, with the modifications listed below.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		423 Interval Too Brief	The SS responds with a 423 (Interval Too Brief) too brief response to the REGISTER request with T value in Min-Expires header.
3	→		REGISTER	UE sends a new REGISTER request with expires parameter value set to Tmod (equal or greater to T value in Min-Expires header of 423 (Interval Too Brief)).
4	←→		Continue with Annex C.2b step 3	Execute the Generic test procedure Annex C.2b steps 3-9 in order to get the UE in a stable registered state.

Specific Message Contents

REGISTER (Step 1)

Use the default message "REGISTER" in annex A.1.1 with condition A14 "Initial REGISTER SIP Digest without TLS for Fixed Broadband Access".

423 Interval Too Brief for REGISTER (Step 2)

Use the default message "423 Interval Too Brief for REGISTER" in annex A.1.7 with the following exception:

Header/param	Value/remark
Min-Expires	
delta-seconds	*800000* (referred to as T in the test procedure and test requirement)

REGISTER (Step 3)

Use the default message "REGISTER" in annex A.1.1 with condition A14 "Initial REGISTER SIP Digest without TLS for Fixed Broadband Access" with the following exceptions:

Header/param	Value/remark
Contact	
expires	*800000* (referred to as Tmod in the expected sequence) (if present, see Rule 1)
Expires	(if present, see Rule 1)
delta-seconds	*800000* (referred to as Tmod in the expected sequence)
CSeq	
value	must be incremented from the previous REGISTER

Rule 1: The REGISTER request must contain either an Expires header or an expires parameter in the Contact header. If both are present the value of Expires header is not important.

Modifications to steps detailed in Appendix C.2b:

REGISTER (Step 4)

Header/param	Value/remark
Contact	
expires	*800000* (if present)
Expires	(if present)
delta-seconds	*800000*

200 OK (Step 5)

Header/param	Value/remark
Contact	
expires	800000

H.8.4.5 Test requirements

Step 3: The UE shall send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

H.8.5 User initiated re-registration - 423 Interval Too Brief / Fixed Broadband Access

H.8.5.1 Definition

As described in clause 8.16.1.

H.8.5.2 Conformance requirement

As described in clause 8.16.2.

H.8.5.3 Test purpose

As described in clause 8.16.3.

H.8.5.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1-8) The same procedures as in subclause H.8.1.4 are used with the exception that the SS sets the expiration time to 120 seconds in Step 4.

9) Before half of the time has expired from the initial registration SS receives re-register message request with the From, To, Via, Contact, Authorization, Expires, Security-Client, Security-verify, Supported, and P-Access-Network-Info header fields.

10) SS responds to the re-register message request with a 423 (Interval Too Brief) response.

11) SS waits for the UE to send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

12) The SS responds to the REGISTER request with a valid 200 OK response indicating the default expiration timeout.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8	←→		Messages in Initial Registration Test case (subclause H.8.1.4)	The same messages as in subclause H.8.1.4 are used with the exception that in Step 4, the SS responds with 200 OK indicating 120 seconds expiration time.
9	→		REGISTER	The SS receives REGISTER from the UE 60 seconds before the expiration time set in the initial registration request.
10	←		423 Interval Too Brief	The SS responds with a 423 (Interval Too Brief) too brief response to the REGISTER request with T value in Min-Expires header.
11	→		REGISTER	UE sends a new REGISTER request with expires parameter value set to Tmod (equal or greater to T value in Min-Expires header of 423 (Interval Too Brief)).
12	←		200 OK	The SS responds with 200 OK indicating the default expiration time.

Specific Message Contents

Messages in Step 1-8

Messages in Step 1-8 are the same as those specified in subclause H.8.1.4 with the following exception for the 200 OK for REGISTER in Step 4:

Use the default message “200 OK for REGISTER” in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	120

REGISTER (Step 9)

Use the default message “REGISTER” in annex A.1.1 with condition A15 "Subsequent REGISTER SIP Digest without TLS for Fixed Broadband Access" and with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, shall be different than in step 3
spi-s	new SPI number of the inbound SA at the protected server port, shall be different than in step 3
port-c	new protected client port, shall be different than in step 3
port-s	Same value as in the previous REGISTER

423 Interval Too Brief for REGISTER (Step 10)

Use the default message "423 Interval Too Brief for REGISTER" in annex A.1.7 with the following exception:

Header/param	Value/remark
Min-Expires	
delta-seconds	*800000* (referred to as T in the test procedure and test requirement)

REGISTER (Step 11)

Use the default message "REGISTER" in annex A.1.1 with condition A14 "Initial REGISTER SIP Digest without TLS for Fixed Broadband Access" with the following exceptions:

Header/param	Value/remark
Contact	
expires	*800000* (referred to as Tmod in the expected sequence) (if present, see Rule 1)
Expires	(if present, see Rule 1)
delta-seconds	*800000* (referred to as Tmod in the expected sequence)
CSeq	
value	must be incremented from the previous REGISTER

Rule 1: The REGISTER request must contain either an Expires header or an expires parameter in the Contact header. If both are present the value of Expires header is not important.

200 OK (Step 12)

Header/param	Value/remark
Contact	
expires	800000

H.8.5.5 Test requirements

Step 11: The UE shall send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

H.9 Authentication

H.9.1 SIP digest without TLS - abnormal procedures - 403 Forbidden / Fixed Broadband Access

H.9.1.1 Definition

Test to verify that On receiving a 403 (Forbidden) response, the UE shall consider the registration to have failed.

H.9.1.2 Conformance requirement

[TS 24.229, 5.1.1.1B.1]:

In case the UE contains neither an ISIM nor a USIM, but IMC is present the UE shall use preconfigured parameters in the IMC to initiate the registration to the IM CN subsystem and for authentication.

The following IMS parameters are assumed to be available to the UE:

- a private user identity;

- a public user identity; and
- a home network domain name to address the SIP REGISTER request to.

These parameters may not necessarily reside in a UICC.

The first public user identity in the list stored in the IMC is used in emergency registration requests.

[TS 24.229 Rel-12, clause 5.1.1.2.1]:

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

When registering any public user identity belonging to the UE, the UE shall either use an already active pair of security associations or a TLS session to protect the REGISTER requests, or register the public user identity via a new initial registration procedure.

When binding any one of its public user identities to an additional contact address via a new initial registration procedure, the UE shall follow the procedures described in RFC 5626 [92]. The set of security associations or a TLS session resulting from this initial registration procedure will have no impact on the existing set of security associations or TLS sessions that have been established as a result of previous initial registration procedures. However, if the UE registers any one of its public user identities with a new contact address via a new initial registration procedure and does not employ the procedures described in RFC 5626 [92], then the new set of security associations or TLS session shall replace any existing set of security association or TLS session.

If the UE detects that the existing security associations or TLS sessions associated with a given contact address are no longer active (e.g., after receiving no response to several protected messages), the UE shall:

- consider all previously registered public user identities bound to this security associations or TLS session that are only associated with this contact address as deregistered; and
- stop processing all associated ongoing dialogs and transactions that were using the security associations or TLS session associated with this contact address, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs).

The UE shall send the unprotected REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, or if the UE was pre-configured with the P-CSCF's IP address or domain name and was unable to obtain specific port information, the UE shall send the unprotected REGISTER request to the SIP default port values as specified in RFC 3261 [26].

NOTE 1: The UE will only send further registration and subsequent SIP messages towards the same port of the P-CSCF for security mechanisms that do not require using negotiated ports for exchanging protected messages.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in clause 5.1.1.1A or clause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains:

1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

2) the public user identity to be registered;

b) a To header field set to the SIP URI that contains:

1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

2) the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE:

1) supports GRUU (see table A.4, item A.4/53);

2) supports multiple registrations;

3) has an IMEI available; or

4) has an MEID available;

the UE shall include a "+sip.instance" header field parameter containing the instance ID. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in clause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in clause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in clause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in clause 7.9.3 and RFC 3840 [62].

if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Contact URI without a user portion and containing the "bnc" URI parameter;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. For the UDP, the UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223 [143];

NOTE 3: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 4: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

1) if GRUU is supported, the option-tag "gruu"; and

2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see clause 7.2A.4);

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in clause 7.2A.7;

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and

k) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

a) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in clause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, the UE may initiate that mechanism on a media level when it initiates new media in an existing session.

NOTE 6: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header field value and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

NOTE 7: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the To header field will contain the main URI of the UE.

b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 8: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;

d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 9: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 10: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions (other than REGISTER method) when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:

- if the UE did not use the procedures specified in RFC 6140 [191] for registration, find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered; and

- if the UE used the procedures specified in RFC 6140 [191] for registration then find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter then store the value of the "pub-gruu" header field parameter for use for generating public GRUUs for registering UAs as specified in RFC 6140 [191]. If this contains a "temp-gruu-cookie" header field parameter then store the value of the "temp-gruu-cookie" header field parameter for use for generating temporary GRUUs for registering UAs as specified in RFC 6140 [191];

NOTE 11: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquely identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in clause 7.1.2.2 of RFC 6140 [191].

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626 [92], and the S-CSCF has followed the registration procedure as described in RFC 5627 [93] or RFC 3261 [26], i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626 [92], the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626 [92]; or

NOTE 12: Upon replaces the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in clause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about the deregistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626 [92];

g) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in clause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session;

NOTE 13: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223 [143];

i) if the 200 (OK) response includes a Feature-Caps header field, as specified in RFC 6809°[190], with "+g.3gpp.icsi-ref" header field parameter, then the UE may consider the values included in the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field of 200 (OK) response as supported by the IM subsystem for the established registration or registration flow (if the multiple registration mechanism is used); and

NOTE 14: The UE and related applications can use the ICSI values received in the Feature-Caps header field of 200 (OK) response to improve the user experience.

j) if the 200 (OK) response includes one or more Feature-Caps header fields containing the capability indicators listed in clause 7.9A.7 that indicate the media capabilities supported by the IMS-AGW then the UE may consider this information when providing media options to the user or determining whether an application communication capability will be successful (e.g. if "sip.video" is not indicated then the UE might not offer the user the option to attempt to add video to the session).

NOTE 15: If media capability indication is not supported, no capability indicators listed in clause 7.9A.7 are included and it can be assumed that all the media capabilities are supported.

On receiving a 305 (Use Proxy) response to the unprotected REGISTER request, unless otherwise specified in access specific annexes (as described in Annex B or Annex L), the UE shall:

a) ignore the contents of the Contact header field if it is included in the received message;

NOTE 16: The 305 response is not expected to contain a Contact header field.

b) release all IP-CAN bearers used for the transport of media according to the procedures in clause 9.2.2;

c) initiate either a new P-CSCF discovery procedure as described in clause 9.2.1, or select a new P-CSCF, if the UE was pre-configured with more than one P-CSCF's IP addresses or domain names;

d) select a P-CSCF address, which is different from the previously used address, from the address list; and

e) perform the procedures for initial registration as described in clause 5.1.1.2.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) or 600 (Busy Everywhere) response for an initial registration, the UE may attempt to perform initial registration again.

When the timer F expires at the UE, the UE may:

a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in clause 9.2.1 or from its pre-configured list of P-CSCF's IP addresses or domain names;

b) if no response has been received when attempting to contact all P-CSCFs known by the UE, get a new set of P-CSCF-addresses as described in clause 9.2.1 unless otherwise specified in the access specific annexes (as described in Annex B or Annex L); and

c) perform the procedures for initial registration as described in clause 5.1.1.2.

NOTE 17: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

On receiving a 4xx, 5xx or 6xx response to the REGISTER request, whereby the response contains a Retry-After header field, the UE shall not automatically attempt an initial registration via the same IP-CAN and the same P-CSCF for the amount of time indicated in the Retry-After header field. If the UE is power cycled, the UE can attempt an initial registration. If no initial registration occurs within the time period indicated by the Retry-After header field, the counter of unsuccessful initial registration attempts is reset.

After a first unsuccessful initial registration attempt, if the Retry-After header field was not present and the initial registration was not performed as a consequence of a failed reregistration, the UE shall not wait more than 5 minutes before attempting a new registration.

After a maximum of 2 consecutive unsuccessful initial registration attempts, if the Retry-After header field was not present in failure responses of those unsuccessful initial registration attempts, the UE shall implement the mechanism defined in clause 4.5 of RFC 5626 [92] for new registration attempts. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in clause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time have been provided to the UE by the network, the default values defined in clause 4.5 of RFC 5626 [92] shall be used.

The values of max-time and base-time may be provided by the network to the UE using OMA-DM with the management objects specified in 3GPP TS 24.167 [8G]. Other mechanisms may be used as well and are outside the scope of the present specification.

[TS 24.229, clause 5.1.1.2.3]:

On sending a REGISTER request, as defined in clause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 [21] unless otherwise specified in the access specific annexes, with:

- the "username" header field parameter, set to the value of the private user identity;

- the "realm" header field parameter, set to the domain name of the home network;

- the "uri" header field directive, set to the SIP URI of the domain name of the home network;

- the "nonce" header field parameter, set to an empty value; and

- the "response" header field parameter, set to an empty value;

b) the hostport parameter in the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent requests; and

c) the sent-by field in the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

The UE shall use the locally available public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration. The method whereby the public user identity and private user identity are made available to the UE is outside the scope of this document (e.g. a public user identity could be input by the end user).

[TS 24.229, 5.1.1.5.5]:

On receiving a 403 (Forbidden) response, the UE shall consider the registration to have failed.

Reference(s)

TS 24.229[10], clauses 5.1.1.1B.1, 5.1.1.2.1, 5.1.1.2.3 and 5.1.1.5.5.

H.9.1.3 Test purpose

To verify that after receiving a 403 (Forbidden) the UE registration fails.

H.9.1.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		403 FORBIDDEN	The SS responds with a 403 FORBIDDEN message including a Retry-After header set to 20 seconds.
3				SS waits 18 seconds

Specific Message Contents

REGISTER (Step 1)

Use the default message "REGISTER" in annex A.1.1 with condition A14 "Initial REGISTER over Fixed Access Broadband".

403 Forbidden (Step 2)

Use the default message “403 Forbidden” in Annex A.3.2 and include a Retry-After header set to 20 seconds.

H.9.1.5 Test requirements

If the UE is preconfigured with the home domain name, public and private user identities and SIP Digest Credentials

Step 1: SS shall check that in accordance to the TS 24.229 [10] clause 5.1.1.3 the UE sends a REGISTER.

Step 3: SS shall check that the UE does not re-attempt an IMS registration within the time period indicated by the Retry-After header field.

H.10 Void

H.11 Notification

H.11.1 Void

H.11.2 Network initiated re-authentication / Fixed Broadband Access

H.11.2.1 Definition

Test to verify that the UE can correctly process a network initiated re-authentication request and re-authenticate the user before the registration expires over Fixed Broadband Access, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5A.

H.11.2.2 Conformance requirement

As described in clause 11.2.2.

H.11.2.3 Test purpose

As described in clause 11.2.3.

H.11.2.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed Digest-MD5 authentication with the UE and accepted the registration.

Test procedure

As described in clause 11.2.4.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing partial registration state information, indicating shortened expiration time (60 seconds) for the registered public user identity in the XML body.
2	→		200 OK	The UE responds the NOTIFY with 200 OK.
3	→		REGISTER	UE re-registers the user 30 seconds before the expected expiration.
4	←		401 Unauthorized	The SS responds with a valid Digest-MD5 authentication challenge.
5	→		REGISTER	UE sends another REGISTER with Digest-MD5 credentials.
6	<-		200 OK	The UE responds with 200 OK.

Specific Message Contents

As described in clause 11.2.4.

NOTE: The default messages contents in Annex A are used with condition “SIP Digest without TLS for Fixed Broadband Access” when applicable.

H.11.2.5 Test requirements

Step 2: SS shall check that the UE sends the 200 OK response.

Step 3: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.4 the UE sends a REGISTER request.

H.12 Call Control

H.12.1 Originating – 503 Service Unavailable / Fixed Broadband Access

H.12.1.1 Definition

When a server is temporarily unable to process an INVITE request due to a temporary overloading or maintenance of the server sends a 503 Service Unavailable response. The server may indicate when the service will be available again in a Retry-After header field. This process is described in 3GPP TS 24.229 [10], clause 5.1.3.1.

H.12.1.2 Conformance requirement

Upon receiving a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the originating UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

Reference(s)

3GPP TS 24.229 [10], clause 5.1.3.1.

H.12.1.3 Test purpose

Verify that UE does not automatically reattempt the request until the period indicated by the Retry-After header contents. When a server is temporarily unable to process an INVITE request due to a temporary overloading or maintenance of the server, sends a 503 Service Unavailable response. The server may indicate when the service will be available again in a Retry-After header field.

H.12.1.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration.

Test procedure

For value of T see specific message content for 503 (Service Unavailable) message specified in Annex A.4.2.

1) The UE initiates and successfully completes IMS registration. as per Annex C.2b.

2) Steps 1-3 of expected sequence as defined in Annex C.21c.

5) The SS responds with a 503 (Service Unavailable) response with the Retry-After header set to T.

6) The SS waits for the UE to send an ACK to acknowledge the reception of the 503 (Service Unavailable) response.

7) SS waits for a duration of time T and checks that the UE does not reattempt sending the INVITE request.

8) After the time T the UE may reattempt sending the INVITE.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-3			Steps 1, 2 and 3 defined in annex C.21c	Originating MTSI voice call over Fixed Broadband Access
4	←		503 Service Unavailable	Including Retry-After header with period set to T
5	→		ACK	The UE acknowledges the reception of the 503 (Service Unavailable) response
6				The SS waits for a duration of time T and checks that the UE does not re-send the INVITE request
7			Step 2 defined in annex C.21c	Optional

Specific Message Contents

Steps 1 - 3 as specified in annex C.21c

503 Service Unavailable (Step 4)

Use the default message “503 Service Unavailable” in annex A.4.2.

H.12.1.5 Test requirements

At step 6 the UE shall not reattempt the INVITE request before time T from the time the SS receives the ACK from the UE in step 5.

H.12.2 Originating – 504 Server Time-out / Fixed Broadband Access

H.12.2.1 Definition

When the S-CSCF is temporarily unable to process an INVITE as the S-CSCF does not have the user profile or does not trust the data that it has (e.g. due to restart), the S-CSCF can reject the request by returning a 504 (Server Time-out) response to the UE with specific content as specified in [10] clause 5.4.3.2. As a result the UE will initiate restoration procedures by performing an initial registration.

H.12.2.2 Conformance requirement

In the event the UE receives a 504 (Server Time-out) response containing:

1) a P-Asserted-Identity header field set to a value equal to a URI:

   a) from the Service-Route header field value received during registration; or

   b) from the Path header field value received during registration; and

2) a Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the default content disposition, identified as "3gpp-alternative-service", is applied as follows:

   a) if the 504 (Server Time-out) response includes an IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element:

      a) with the <type> child element set to "restoration" (see table 7.7AA); and

      b) with the <action> child element set to "initial-registration" (see table 7.7AB);

      then the UE:

      - shall initiate restoration procedures by performing an initial registration as specified in subclause 5.1.1.2; and

- may provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

Reference(s)

3GPP TS 24.229[10], clause 5.1.2A.1.6

H.12.2.3 Test purpose

To verify that when the UE receives a 504 (Server Time-out) response to an INVITE request containing a P-Asserted-Identity header field set to a value equal to a URI from the Service-Route header field value received during registration and the rest of the message is set as described in [10] subclause 5.1.2A.1.6, then the UE initiates restoration procedures by performing an initial registration as specified in [10] subclause 5.1.1.2.

H.12.2.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration.

Test procedure applicable

1) The UE initiates and successfully completes IMS registration. as per Annex C.2b.

2) Steps 1-3 of expected sequence as defined in Annex C.21b.

5) The SS responds with a 504 (Server Time-out) response.

6) The SS waits for the UE to send an ACK to acknowledge the reception of the 504 (Server Time-out) response.

7-14) As specified in steps 4-11 annex C.2b.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-2			Steps 1-2 defined in annex C.21b	Originating MTSI voice call over Fixed Broadband Access
3	←		504 Server Time-out	Set as per the specific message contents.
4	→		ACK	The UE acknowledges the reception of the 504 (Server Time-out) response
5-12			Step 2 defined in annex C.2b	The UE performs an initial registration

Specific Message Contents

Steps 1 - 2 as specified in annex C.21b

504 Server Time-out (Step 3)

Use the default message “504 Server Time-out” in Annex A.4.6

ACK (Step 4)

As specified in annex A.2.7.

Steps 5-12

As specified in annex C.2b

H.12.2.5 Test requirements

After step 3 the UE shall perform an initial registration.

H.12.3 Originating MTSI Voice Call Successful with preconditions / Fixed Broadband Access

H.12.3.1 Definition

Test to verify that the UE correctly performs IMS UE originated voice call setup and release when using IMS Multimedia Telephony with preconditions.

H.12.3.2 Conformance requirement

[TS 24.229, clause 5.1.2A.1]:

If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

When SIP digest is in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;
- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;
- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used); and
- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

[TS 24.229, clause 5.1.2A.1.2]:

The UE may use non-international formats of E.164 addresses, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

Local numbering information is sent in the Request-URI in initials requests or stand alone transaction, using one of the following formats:

1) a tel-URI, complying with RFC 3966, with a local number followed by a "phone-context" tel URI parameter value.
2) a SIP URI, complying with RFC 3261, with the "user" SIP URI parameter set to "phone"
3) a SIP URI, complying with RFC 3261 and RFC 4967, with the "user" SIP URI parameter set to "dialstring"

The actual value of the URI depends on whether user equipment performs an analysis of the dial string input by the end user or not.

[TS 24.229, clause 5.1.2A.1.5]:

When the UE uses home-local number, the UE shall include in the "phone-context" tel URI parameter the home domain name in accordance with RFC 3966.

When the UE uses geo-local number, the UE shall:

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header field into the request), include the access technology information in the "phone-context" tel URI parameter according to RFC 3966 as defined in subclause 7.2A.10; and
- if access technology information is not available to the UE (i.e., the UE cannot insert P-Access-Network-Info header field into the request), include in the "phone-context" tel URI parameter the home domain name prefixed by the "geo-local." string according to RFC 3966 as defined in subclause 7.2A.10.

When the UE uses other local numbers, than geo-local number or home local numbers , e.g. private numbers that are different from home-local number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966, e.g. if private numbers are used a domain name to which the private addressing plan is associated.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value inserted by the UE, based on implementation.

NOTE 2: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is implementation specific.

NOTE 3: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

[TS 24.229, clause 5.1.3.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

The precondition mechanism should be supported by the originating UE.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources, an originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and
- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

Upon generating an initial INVITE request using the precondition mechanism, the UE should not indicate the requirement for the precondition mechanism by using the Require header mechanism.

NOTE 2: If an UE chooses to require the precondition mechanism, i.e. if it indicates the "precondition" option tag within the Require header, the interworking with a remote UE, that does not support the precondition mechanism, is not described in this specification.

NOTE 3: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 4: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation, in case the terminating UE does not support the PRACK request (as described in RFC 3262) and does not support the UPDATE request (as described in RFC 3311).

....

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and
2) send a BYE request to this dialog in order to terminate it.

[TS 24.229, clause 6.1.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,
- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566, unless the UE knows that the precondition mechanism is supported by the remote UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 and RFC 4032; and
- the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec for one or more media streams, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A.1, 5.1.2A.1.2, 5.1.2A.1.5, 5.1.3.1, 6.1.1 and 6.12.

H.12.3.3 Test purpose

1) To verify that when Originating a Voice call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and
2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media and indicating preconditions for optional resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1).
3) To verify that the UE is able to release the call.

H.12.3.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.21b	MTSI Originating speech call.
13A			The UE is triggered by MMI to release the call	
14	→		BYE	The UE releases the call with BYE
15	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Steps 1 - 13 as specified in annex C.21b

BYE (Step 14)

Use the default message "BYE" in annex A.2.8.

200 OK for BYE (Step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

H.12.3.5 Test requirements

SS must check that if the UE uses SIP Digest and it sends all the requests in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 14: the UE shall send a BYE request with the correct content, according to common message definitions.

H.12.4 Originating MTSI Voice call without preconditions / Fixed Broadband Access

H.12.4.1 Definition

Test to verify that the UE correctly performs IMS UE originated voice call setup and release when using IMS Multimedia Telephony without preconditions.

H.12.4.2 Conformance requirement

[TS 24.229, clause 5.1.2A.1]:

If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

When SIP digest is in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;
- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;
- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used); and
- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

[TS 24.229, clause 5.1.2A.1.2]:

The UE may use non-international formats of E.164 addresses, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

Local numbering information is sent in the Request-URI in initials requests or stand alone transaction, using one of the following formats:

1) a tel-URI, complying with RFC 3966, with a local number followed by a "phone-context" tel URI parameter value.

2) a SIP URI, complying with RFC 3261, with the "user" SIP URI parameter set to "phone"

3) a SIP URI, complying with RFC 3261 and RFC 4967, with the "user" SIP URI parameter set to "dialstring"

The actual value of the URI depends on whether user equipment performs an analysis of the dial string input by the end user or not.

[TS 24.229, clause 5.1.2A.1.5]:

When the UE uses home-local number, the UE shall include in the "phone-context" tel URI parameter the home domain name in accordance with RFC 3966.

When the UE uses geo-local number, the UE shall:

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header field into the request), include the access technology information in the "phone-context" tel URI parameter according to RFC 3966 as defined in subclause 7.2A.10; and

- if access technology information is not available to the UE (i.e., the UE cannot insert P-Access-Network-Info header field into the request), include in the "phone-context" tel URI parameter the home domain name prefixed by the "geo-local." string according to RFC 3966 as defined in subclause 7.2A.10.

When the UE uses other local numbers, than geo-local number or home local numbers , e.g. private numbers that are different from home-local number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966, e.g. if private numbers are used a domain name to which the private addressing plan is associated.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value inserted by the UE, based on

implementation.

NOTE 2: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is implementation specific.

NOTE 3: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

[TS 24.229, clause 5.1.3.1]:

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and

- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

....

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it.

[TS 24.229, clause 6.1.1]:

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

…

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A.1, 5.1.2A.1.2, 5.1.2A.1.5, 5.1.3.1, 6.1.1 and 6.12.

H.12.4.3 Test purpose

1) To verify that when Originating a Voice call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media (as described by 3GPP TS 24.229 [10], clause 6.1).

3) To verify that the UE is able to release the call.

H.12.4.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration.

Test procedure

1-9) UE executes the procedures defined in annex C.2b steps 1 to 9.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.21c	MTSI Originating speech call.
9			The UE is triggered by MMI to release the call	
10	→		BYE	The UE releases the call with BYE
11	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition “SIP Digest without TLS for Fixed Broadband Access” when applicable

Specific Message Contents

Steps 1 - 8 as specified in annex C.21c

BYE (Step 10)

Use the default message “BYE” in annex A.2.8.

200 OK for BYE (Step 11)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1.

H.12.4.5 Test requirements

SS must check that if the UE uses SIP Digest and it sends all the requests in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 10: the UE shall send a BYE request with the correct content, according to common message definitions.

H.12.5 Terminating MTSI Voice call with preconditions / Fixed Broadband Access

H.12.5.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated speech call setup when using IMS Multimedia Telephony with preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.2A.2 and 5.1.4.1. The test case is applicable for Fixed Broadband Access.

H.12.5.2 Conformance requirement

[TS 24.229, clause 5.1.2A.2]:

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

Where a security association or TLS session exists, the UE shall discard any SIP request that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

If an initial request contains an Accept-Contact header field containing the g.3gpp.icsi-ref media feature tag with an ICSI value, the UE should invoke the IMS application that is the best match for the ICSI value.

If an initial request contains an Accept-Contact header field containing the g.3gpp.iari-ref media feature tag with an IARI value the UE should invoke the IMS application that is the best match for the IARI value.

The UE can receive multiple ICSI values, IARI values or both in an Accept-Contact header field. In this case it is up to the implementation which of the multiple ICSI values or IARI values the UE takes action on.

NOTE 1: The application verifies that the contents of the request (e.g. SDP media capabilities, Content-Type header field) are consistent with the ICSI value in the g.3gpp.icsi-ref media feature tag and IARI value contained in the g.3gpp.iari-ref media feature tag.

If an initial request does not contain an Accept-Contact header field containing a g.3gpp.icsi-ref media feature tag or a g.3gpp.iari-ref media feature tag the UE shall invoke the application that is the best match based on the contents of the request (e.g. SDP media capabilities, Content-Type header field, media feature tag).

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 2: In the UE-terminating case, this version of the document makes no provision for the UE to provide a P-Preferred-Identity in the form of a hint.

NOTE 3: A number of header fields can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 4: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g. first contacted via a registration or configuration procedure). Including the "+sip.instance" header field parameter containing an IMEI URN does not violate RFC 7254 [153] even when the UE requests privacy using RFC 3323 [33].

If the response includes a Contact header field, and the response is sent within an existing dialog, and the Contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header field as specified in RFC 5627 [93].

…

NOTE 5: The above items 1 and 2 are mutually exclusive.

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3841 [56B] the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service and then the UE may include the IARI value for any IMS application that applies for the dialog, (coded as specified in subclause 7.2A.9.2), that is related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B]. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the originating UE(s) and other IARI values for the IMS application that is related to the IMS communication service; and

4) if the request is related to an IMS application that is supported by the UE when the use of an ICSI is not needed, then the UE may include the IARI value (coded as specified in subclause 7.2A.9.2), that is related to any IMS application and that applies for the dialog, in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B].

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

If the UE did not insert a GRUU in the Contact header field then the UE shall include a port in the address in the Contact header field as follows:

- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; or

- if SIP digest without TLS is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial registration.

If the UE receives a Resource-Priority header field in accordance with RFC 4412 [16] in an initial request for a dialog, then the UE shall include the Resource-Priority header field in all requests associated with that dialog.

NOTE 6: For certain national implementations, signalling of a Resource-Priority header field to and from a UE is not required.

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method (see subclause 7.2A.4).

The UE shall not support RFC 7090 [209] (see table A.4, item A.4/116) and, in this version of the specification, the UE shall not perform any specific procedures beyond those defined in RFC 3261 [26] for the Priority header field.

NOTE 7: The mechanism specified in RFC 7090 [209] is based on the presence of a trust domain for the Priority header field in the operator's network. The UE is not aware whether a trust domain for the Priority header field exists in the operator's network.

[TS 24.229, clause 5.1.4.1]:

The preconditions mechanism should be supported by the terminating UE.

The handling of incoming initial INVITE requests at the terminating UE is mainly dependent on the following conditions:

- the specific service requirements for "integration of resource management and SIP" extension (hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by RFC 4032 [64], and with the request for such a mechanism known as a precondition); and

- the UEs configuration for the case when the specific service does not require the precondition mechanism.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header field with the "precondition" option-tag in responses that include SDP body or subsequent requests that include SDP body that it sends towards to the originating UE; or

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism.

If local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field and:

  - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism and shall indicate a Require header field with the "precondition" option-tag in responses that include SDP body or subsequent requests that include SDP body that it sends towards to the originating UE; or

  - the required local resources at the originating UE and the terminating UE are available, the terminating UE may use the precondition mechanism;

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism; or

c) the received INVITE request includes the "precondition" option-tag in the Require header field, the terminating UE shall use the precondition mechanism.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].

NOTE 3: If the terminating UE does not support the precondition mechanism it will apply regular SIP session initiation procedures.

If the terminating UE requires a reliable alerting indication at the originating side, the UE shall send the 180 (Ringing) response reliably. If the received INVITE request indicated support for reliable provisional responses, but did not require their use, the terminating UE shall send provisional responses reliably only if the provisional response carries SDP or for other application related purposes that requires its reliable transport.

NOTE 4: Certain applications, services and operator policies might mandate the terminating UE to send a 199 (Early Dialog Terminated) provisional response (see RFC 6228 [142]) prior to sending a non-2xx final response to the INVITE request.

If the terminating UE uses the precondition mechanism, upon successful reservation of local resources:

- if the originating side requested confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE, the terminating UE shall confirm the successful resource reservation (see subclause 6.1.3) within an SIP UPDATE request; and

NOTE 5: Originating side requests confirmation for the result of the resource reservation at the terminating UE e.g. when an application server performs 3rd party call control. The request for confirmation for the result of the resource reservation at the terminating UE can be included e.g. in the SDP answer in the PRACK request.

- if the originating side did not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE, the terminating UE shall not confirm the successful resource reservation (see subclause 6.1.3) within an UPDATE request.

NOTE 6: The terminating UE can send an UPDATE request for reasons other than confirmation of the successful resource reservation.

If the terminating UE included an SDP offer or an SDP answer in a reliable provisional response to the INVITE request and both the terminating UE and the originating UE support UPDATE method, then in order to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sends an UPDATE request with a new SDP offer and delays sending of 200 (OK) response to the INVITE request till after reception of 200 (OK) response to the UPDATE request.

[TS 24.229, clause 6.1.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

[TS 24.229, clause 6.1.3]:

When the BGCF receives an INVITE request that contains a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter, the BGCF shall decide based on local policy whether to perform loopback routeing for this request. The BGCF shall:

a) if loopback routeing is not to be performed for this request remove any "+g.3gpp.trf" or "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field of the outgoing request;

b) if loopback routeing is applied for this request:

i) remove all entries in the Route header field;

ii) if a "+g.3gpp.trf" header field parameter with a parameter value containing a valid URI, is included in the Feature-Caps header field of the request, insert the URI in a Route header field;

iii) if a "+g.3gpp.trf" header field parameter, with a parameter value containing a valid URI is not included in the Feature-Caps header field of the request, insert a locally configured TRF address, associated with the visited network for this call (as identified in the "+g.3gpp.home-visited" header field parameter), in the Route header field;

iv) remove any "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field of the outgoing request;

v) if included in the incoming request, remove the "+g.3gpp.trf" header field parameter from the Feature-Caps header field from the outgoing request;

vi) insert the "+g.3gpp.loopback" header field parameter, as specified in subclause 7.9A.4 in the Feature-Caps header field of the request, in accordance with RFC 6809 [190]. If providing the identifier of the home network is supported by the BGCF and the visited network, the BGCF may based on operator agreement insert the "+g.3gpp.loopback" header field parameter set to the identifier of the home network;

vii) remove the "orig-ioi" header field parameter received in the P-Charging-Vector header field, if present. The BGCF shall insert a type 1 "orig-ioi" header field parameter into the P-Charging-Vector header field and shall set the type 1 "orig-ioi" header field parameter to a value that identifies the home network of the served user (i.e. the network in which the BGCF resides). The BGCF shall not include the "term-ioi" header field parameter; and

viii) if the BGCF supports indicating the traffic leg associated with a URI as specified in RFC 7549 [225] and if an "iotl" SIP URI parameter is not included in the TRF URI in the Route header field, the BGCF if required by local policy, append an "iotl" URI parameter with a value set to "homeA-visitedA" to the URI in the Route header field; and

c) if the final decision on loopback routeing is deferred to a subsequent entity in the home network, a further BGCF, then, retain in the request a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter with the parameter value set to the identifier of the visited network. The BGCF is expected to know by means of network configuration that such a subsequent entity exists;

If the BGCF inserts its own Record-Route header field, the BGCF may require the periodic refreshment of the session to avoid hung states in the BGCF. If the BGCF requires the session to be refreshed, the BGCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

If overlap signalling using the multiple-INVITE method is supported as a network option, several INVITE requests with the same Call ID and the same From header field (including "tag" header field parameter) can be received outside of an existing dialog. Such INVITE requests relate to the same call and the BGCF shall route such INVITE request received during a certain period of time to the same next hop.

If the BGCF inserted in the initial request for the dialog the header field parameters into the Feature-Caps header field then the BGCF shall include the header field parameters with the same parameter values into the Feature-Caps header field in any target refresh request for the dialog, and in each 1xx or 2xx response to target refresh request sent in the same direction.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A.2, 5.1.4.1, 6.1.1 and 6.1.3.

H.12.5.3 Test purpose

1) To verify that, when initiating Terminating MTSI Voice call and UE needs to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

H.12.5.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure

1-9) UE executes the procedures defined in annex C.2b steps 1 to 9.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.11b	MTSI Terminating speech call over Fixed Broadband Access.

NOTE: The default messages contents in annex A are used with condition “SIP Digest without TLS for Fixed Broadband Access” when applicable

Specific Message Content

None.

H.12.5.5 Test requirements

The UE shall send requests and responses as described in clause H.12.5.4.

H.12.6 Terminating MTSI Voice call without preconditions / Fixed Broadband Access

H.12.6.1 Definition

Test to verify that the UE correctly performs IMS fixed access terminated voice call setup when using IMS Multimedia Telephony without preconditions.

H.12.6.2 Conformance requirement

[TS 24.229, clause 5.1.2A.1]:

If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

When SIP digest is in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;

- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;
- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used); and
- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

[TS 24.229, clause 5.1.2A.2]:

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

Where a security association or TLS session exists, the UE shall discard any SIP request that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

If an initial request contains an Accept-Contact header field containing the g.3gpp.icsi-ref media feature tag with an ICSI value, the UE should invoke the IMS application that is the best match for the ICSI value.

If an initial request contains an Accept-Contact header field containing the g.3gpp.iari-ref media feature tag with an IARI value the UE should invoke the IMS application that is the best match for the IARI value.

The UE can receive multiple ICSI values, IARI values or both in an Accept-Contact header field. In this case it is up to the implementation which of the multiple ICSI values or IARI values the UE takes action on.

NOTE 1: The application verifies that the contents of the request (e.g. SDP media capabilities, Content-Type header field) are consistent with the ICSI value in the g.3gpp.icsi-ref media feature tag and IARI value contained in the g.3gpp.iari-ref media feature tag.

If an initial request does not contain an Accept-Contact header field containing a g.3gpp.icsi-ref media feature tag or a g.3gpp.iari-ref media feature tag the UE shall invoke the application that is the best match based on the contents of the request (e.g. SDP media capabilities, Content-Type header field, media feature tag).

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 2: In the UE-terminating case, this version of the document makes no provision for the UE to provide a P-Preferred-Identity in the form of a hint.

NOTE 3: A number of header fields can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 4: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g. first contacted via a registration or configuration procedure). Including the "+sip.instance" header field parameter containing an IMEI URN does not violate RFC 7254 [153] even when the UE requests privacy using RFC 3323 [33].

If the response includes a Contact header field, and the response is sent within an existing dialog, and the Contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header field as specified in RFC 5627 [93].

…

NOTE 5: The above items 1 and 2 are mutually exclusive.

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3841 [56B] the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service and then the UE may include the IARI value for any IMS application that applies for the dialog, (coded as specified in subclause 7.2A.9.2), that is related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B]. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the originating UE(s) and other IARI values for the IMS application that is related to the IMS communication service; and

4) if the request is related to an IMS application that is supported by the UE when the use of an ICSI is not needed, then the UE may include the IARI value (coded as specified in subclause 7.2A.9.2), that is related to any IMS application and that applies for the dialog, in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B].

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

If the UE did not insert a GRUU in the Contact header field then the UE shall include a port in the address in the Contact header field as follows:

- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; or

- if SIP digest without TLS is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial registration.

If the UE receives a Resource-Priority header field in accordance with RFC 4412 [16] in an initial request for a dialog, then the UE shall include the Resource-Priority header field in all requests associated with that dialog.

NOTE 6: For certain national implementations, signalling of a Resource-Priority header field to and from a UE is not required.

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method (see subclause 7.2A.4).

The UE shall not support RFC 7090 [209] (see table A.4, item A.4/116) and, in this version of the specification, the UE shall not perform any specific procedures beyond those defined in RFC 3261 [26] for the Priority header field.

NOTE 7: The mechanism specified in RFC 7090 [209] is based on the presence of a trust domain for the Priority header field in the operator's network. The UE is not aware whether a trust domain for the Priority header field exists in the operator's network.

[TS 24.229, clause 5.1.4.1]:

The handling of incoming initial INVITE requests at the terminating UE is mainly dependent on the following conditions:

- the specific service requirements for "integration of resource management and SIP" extension (hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by RFC 4032 [64], and with the request for such a mechanism known as a precondition); and

- the UEs configuration for the case when the specific service does not require the precondition mechanism.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header field with the "precondition" option-tag in responses that include SDP body or subsequent requests that include SDP body that it sends towards to the originating UE; or

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism.

If local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field and:

- the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism and shall indicate a Require header field with the "precondition" option-tag in responses that include SDP body or subsequent requests that include SDP body that it sends towards to the originating UE; or

- the required local resources at the originating UE and the terminating UE are available, the terminating UE may use the precondition mechanism;

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism; or

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].

NOTE 3: If the terminating UE does not support the precondition mechanism it will apply regular SIP session initiation procedures.

If the terminating UE requires a reliable alerting indication at the originating side, the UE shall send the 180 (Ringing) response reliably. If the received INVITE request indicated support for reliable provisional responses, but did not require their use, the terminating UE shall send provisional responses reliably only if the provisional response carries SDP or for other application related purposes that requires its reliable transport.

NOTE 4: Certain applications, services and operator policies might mandate the terminating UE to send a 199 (Early Dialog Terminated) provisional response (see RFC 6228 [142]) prior to sending a non-2xx final response to the INVITE request.

…..

If the terminating UE included an SDP offer or an SDP answer in a reliable provisional response to the INVITE request and both the terminating UE and the originating UE support UPDATE method, then in order to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sends an UPDATE request with a new SDP offer and delays sending of 200 (OK) response to the INVITE request till after reception of 200 (OK) response to the UPDATE request.

[TS 24.229, clause 6.1.1]:

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A.2, 5.1.4.1 and 6.1.1.

H.12.6.3 Test purpose

1) To verify that when Terminating a Voice call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media (as described by 3GPP TS 24.229 [10], clause 6.1).

3) To verify that the UE is able to release the call.

H.12.6.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test procedure applicable

1-9) UE executes the procedures defined in annex C.2b steps 1 to 9.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-10			Steps defined in annex C.11c	MTSI Terminating speech call over Fixed Broadband Access.

NOTE: The default messages contents in annex A are used with condition “SIP Digest without TLS for Fixed Broadband Access” when applicable

Specific Message Content

None.

H.12.6.5 Test requirements

SS must check that if the UE uses SIP Digest and it sends all the requests in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

The UE shall send requests and responses as described in clause H.12.6.4.

H.12.7 Originating MTSI Video call without preconditions / Fixed Broadband Access

H.12.7.1 Definition

Test to verify that the UE correctly performs IMS UE originated video call setup and release when using IMS Multimedia Telephony without preconditions. The test case is applicable for SIP Digest without TLS.

H.12.7.2 Conformance requirement

[TS 24.229, clause 5.1.2A.1]:

If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

When SIP digest is in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;
- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;
- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used); and
- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

[TS 24.229, clause 5.1.2A.1.2]:

The UE may use non-international formats of E.164 addresses, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

Local numbering information is sent in the Request-URI in initials requests or stand alone transaction, using one of the following formats:

1) a tel-URI, complying with RFC 3966, with a local number followed by a "phone-context" tel URI parameter value.
2) a SIP URI, complying with RFC 3261, with the "user" SIP URI parameter set to "phone"
3) a SIP URI, complying with RFC 3261 and RFC 4967, with the "user" SIP URI parameter set to "dialstring"

The actual value of the URI depends on whether user equipment performs an analysis of the dial string input by the end user or not.

[TS 24.229, clause 5.1.2A.1.5]:

When the UE uses home-local number, the UE shall include in the "phone-context" tel URI parameter the home domain name in accordance with RFC 3966.

When the UE uses geo-local number, the UE shall:

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header field into the request), include the access technology information in the "phone-context" tel URI parameter according to RFC 3966 as defined in subclause 7.2A.10; and
- if access technology information is not available to the UE (i.e., the UE cannot insert P-Access-Network-Info header field into the request), include in the "phone-context" tel URI parameter the home domain name prefixed by the "geo-local." string according to RFC 3966 as defined in subclause 7.2A.10.

When the UE uses other local numbers, than geo-local number or home local numbers , e.g. private numbers that are different from home-local number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966, e.g. if private numbers are used a domain name to which the private addressing plan is associated.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value inserted by the UE, based on

implementation.

NOTE 2: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is implementation specific.

NOTE 3: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

[TS 24.229, clause 5.1.3.1]:

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and
- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

...

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and
2) send a BYE request to this dialog in order to terminate it.

[TS 24.229, clause 6.1.1]:

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

…

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A.1, 5.1.2A.1.2, 5.1.2A.1.5, 5.1.3.1, 6.1.1 and 6.12.

H.12.7.3 Test purpose

1) To verify that when Originating a Video call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media (as described by TS 24.229 [10], clause 6.1).

3) To verify that the UE is able to release the call.

H.12.7.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.25b	MTSI Originating Video call.
9			The UE is triggered by MMI to release the call	
10	->		BYE	The UE releases the call with BYE
11	<-		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition "SIP Digest without TLS for Fixed Broadband Access" when applicable.

Specific Message Contents

Steps 1 - 8 as specified in annex C.25b.

BYE (Step 10)

Use the default message "BYE" in annex A.2.8.

200 OK for BYE (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

H.12.7.5 Test requirements

SS must check that if the UE uses SIP Digest and it sends all the requests in accordance to TS 24.229 [10], clause 5.1.1.5.1.

Step 10: the UE shall send a BYE request with the correct content, according to common message definitions.

H.12.8 Terminating MTSI Video call without preconditions / Fixed Broadband Access

H.12.8.1 Definition

Test to verify that the UE correctly performs IMS fixed access terminated video call setup when using IMS Multimedia Telephony without preconditions.

H.12.8.2 Conformance requirement

[TS 24.229, clause 5.1.2A.1]:

If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

When SIP digest is in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;
- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;
- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used); and
- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

[TS 24.229, clause 5.1.2A.2]:

The procedures of this clause are general to all requests and responses, except those for the REGISTER method.

Where a security association or TLS session exists, the UE shall discard any SIP request that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in clause 5.1.1.

If an initial request contains an Accept-Contact header field containing the g.3gpp.icsi-ref media feature tag with an ICSI value, the UE should invoke the IMS application that is the best match for the ICSI value.

If an initial request contains an Accept-Contact header field containing the g.3gpp.iari-ref media feature tag with an IARI value the UE should invoke the IMS application that is the best match for the IARI value.

The UE can receive multiple ICSI values, IARI values or both in an Accept-Contact header field. In this case it is up to the implementation which of the multiple ICSI values or IARI values the UE takes action on.

NOTE 1: The application verifies that the contents of the request (e.g. SDP media capabilities, Content-Type header field) are consistent with the ICSI value in the g.3gpp.icsi-ref media feature tag and IARI value contained in the g.3gpp.iari-ref media feature tag.

If an initial request does not contain an Accept-Contact header field containing a g.3gpp.icsi-ref media feature tag or a g.3gpp.iari-ref media feature tag the UE shall invoke the application that is the best match based on the contents of the request (e.g. SDP media capabilities, Content-Type header field, media feature tag).

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 2: In the UE-terminating case, this version of the document makes no provision for the UE to provide a P-Preferred-Identity in the form of a hint.

NOTE 3: A number of header fields can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] clause 4.1 gives considerations relating to a number of header fields.

The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 4: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g. first contacted via a registration or configuration procedure). Including the "+sip.instance" header field parameter containing an IMEI URN does not violate RFC 7254 [153] even when the UE requests privacy using RFC 3323 [33].

If the response includes a Contact header field, and the response is sent within an existing dialog, and the Contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header field as specified in RFC 5627 [93].

…

NOTE 5: The above items 1 and 2 are mutually exclusive.

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag as defined in clause 7.9.2 and RFC 3841 [56B] the ICSI value (coded as specified in clause 7.2A.8.2), for the IMS communication service and then the UE may include the IARI value for any IMS application that applies for the dialog, (coded as specified in clause 7.2A.9.2), that is related to the request in a g.3gpp.iari-ref media feature tag as defined in clause 7.9.3 and RFC 3841 [56B]. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the originating UE(s) and other IARI values for the IMS application that is related to the IMS communication service; and

4) if the request is related to an IMS application that is supported by the UE when the use of an ICSI is not needed, then the UE may include the IARI value (coded as specified in clause 7.2A.9.2), that is related to any IMS application and that applies for the dialog, in a g.3gpp.iari-ref media feature tag as defined in clause 7.9.3 and RFC 3841 [56B].

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

If the UE did not insert a GRUU in the Contact header field then the UE shall include a port in the address in the Contact header field as follows:

- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; or
- if SIP digest without TLS is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial registration.

If the UE receives a Resource-Priority header field in accordance with RFC 4412 [16] in an initial request for a dialog, then the UE shall include the Resource-Priority header field in all requests associated with that dialog.

NOTE 6: For certain national implementations, signalling of a Resource-Priority header field to and from a UE is not required.

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method (see clause 7.2A.4).

The UE shall not support RFC 7090 [209] (see table A.4, item A.4/116) and, in this version of the specification, the UE shall not perform any specific procedures beyond those defined in RFC 3261 [26] for the Priority header field.

NOTE 7: The mechanism specified in RFC 7090 [209] is based on the presence of a trust domain for the Priority header field in the operator's network. The UE is not aware whether a trust domain for the Priority header field exists in the operator's network.

[TS 24.229, clause 5.1.4.1]:

The handling of incoming initial INVITE requests at the terminating UE is mainly dependent on the following conditions:

- the specific service requirements for "integration of resource management and SIP" extension (hereafter in this clause known as the precondition mechanism and defined in RFC 3312 [30] as updated by RFC 4032 [64], and with the request for such a mechanism known as a precondition); and

- the UEs configuration for the case when the specific service does not require the precondition mechanism.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header field with the "precondition" option-tag in responses that include SDP body or subsequent requests that include SDP body that it sends towards to the originating UE; or

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism.

If local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field and:

- the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism and shall indicate a Require header field with the "precondition" option-tag in responses that include SDP body or subsequent requests that include SDP body that it sends towards to the originating UE; or

- the required local resources at the originating UE and the terminating UE are available, the terminating UE may use the precondition mechanism;

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].

NOTE 3: If the terminating UE does not support the precondition mechanism it will apply regular SIP session initiation procedures.

If the terminating UE requires a reliable alerting indication at the originating side, the UE shall send the 180 (Ringing) response reliably. If the received INVITE request indicated support for reliable provisional responses, but did not require their use, the terminating UE shall send provisional responses reliably only if the provisional response carries SDP or for other application related purposes that requires its reliable transport.

NOTE 4: Certain applications, services and operator policies might mandate the terminating UE to send a 199 (Early Dialog Terminated) provisional response (see RFC 6228 [142]) prior to sending a non-2xx final response to the INVITE request.

…..

If the terminating UE included an SDP offer or an SDP answer in a reliable provisional response to the INVITE request and both the terminating UE and the originating UE support UPDATE method, then in order to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sends an UPDATE request with a new SDP offer and delays sending of 200 (OK) response to the INVITE request till after reception of 200 (OK) response to the UPDATE request.

[TS 24.229, clause 6.1.1]:

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in clause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see clause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

Reference(s)

TS 24.229[10], clauses 5.1.2A.2, 5.1.4.1 and 6.1.1.

H.12.8.3 Test purpose

1) To verify that when Terminating a Video call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media (as described by TS 24.229 [10], clause 6.1).

3) To verify that the UE is able to release the call.

H.12.8.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to TS 33.203 [14] clause 6.1 and RFC 3310 [17].

1-9) UE executes the procedures defined in annex C.2b steps 1 to 9.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.25b	Originating MTSI Video Call over Fixed Broadband Access.

NOTE: The default messages contents in annex A are used with condition "SIP Digest without TLS for Fixed Broadband Access" when applicable.

Specific Message Content

None.

H.12.8.5 Test requirements

SS must check that if the UE uses SIP Digest and it sends all the requests in accordance to TS 24.229 [10], clause 5.1.1.5.1.

The UE shall send requests and responses as described in clause H.12.8.4.

H.13 to H.14 Void

H.15 Supplementary Services

H.15.1 Originating Identification Presentation / Fixed Broadband Access

H.15.1.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Originating Identification Presentation. This process is described in 3GPP TS 24.607 [102].

H.15.1.2 Conformance requirement

As described in clause 15.1.2.

H.15.1.3 Test purpose

As described in clause 15.1.3.

H.15.1.4 Method of test

Initial conditions

UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN with xDSL, Fiber or Ethernet with SS. SS is configured with the HTTP Digest password for XCAP, related to the IMS private user identity (IMPI) configured on the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Originating Identification Presentation, at step 7 deactivation of Originating Identification Presentation is respectively triggered at the UE.

H.15.1.5 Test requirements

As described in clause 15.1.5.

H.15.2 Originating Identification Restriction / Fixed Broadband Access

H.15.2.1 Definition

Test to verify that the UE correctly invokes the IMS Multimedia Telephony Originating Identification Restriction. This process is described in 3GPP TS 24.607 [102].

H.15.2.2 Conformance requirement

As described in clause 15.2a.2.

H.15.2.3 Test purpose

As described in clause 15.2a.3.

H.15.2.4 Method of test

Initial conditions

Same as clause H.12.1 with the following addition:

The UE is configured for Originating Identification Restriction

Test procedure

As described in clause 15.2a.4, steps 1-14. Except, steps 2-13 replaced by steps 1-8 in C.21b.

H.15.2.5 Test requirements

As described in clause 15.2a.5.

H.15.3 Terminating Identification Presentation / Fixed Broadband Access

H.15.3.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Terminating Identification Presentation. This process is described in 3GPP TS 24.608 [103].

H.15.3.2 Conformance requirement

As described in clause 15.3.2.

H.15.3.3 Test purpose

As described in clause 15.3.3.

H.15.3.4 Method of test

Initial conditions

UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN with xDSL, Fiber or Ethernet with SS. SS is configured with the HTTP Digest password for XCAP, related to the IMS private user identity (IMPI) configured on the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Terminating Identification Presentation, at step 7 deactivation of Terminating Identification Presentation is respectively triggered at the UE.

H.15.3.5 Test requirements

As described in clause 15.3.5.

H.15.4 Terminating Identification Restriction / Fixed Broadband Access

H.15.4.1 Definition

Test to verify that the UE correctly invokes the IMS Multimedia Telephony Terminating Identification Restriction. This process is described in 3GPP TS 24.608 [103].

H.15.4.2 Conformance requirement

As described in clause 15.4a.2.

H.15.4.3 Test purpose

As described in clause 15.4a.3.

H.15.4.4 Method of test

Initial conditions

Same as clause H.12.6 with the following addition:

The UE is configured for Terminating Identification Restriction

Test procedure

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-5			Steps 1-5 defined in annex C.11c	MTSI MT speech call.
6				Make UE accept the speech offer with Terminating Identification Restriction
7-8			Steps 7-8 defined in annex C.11c	MTSI MT speech call.

Specific Message Contents

180 Ringing (Step 3)

Use the default message “180 Ringing for INVITE” in annex A.2.6 with the following exceptions:

Header/param	Value/remark	Reference
Privacy	*id*	RFC 3323 [135] RFC 3325 [136]

200 Ok (Step 7)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark	Reference
Privacy	*id*	RFC 3323 [135] RFC 3325 [136]

H.15.4.5 Test requirements

The UE shall send requests and responses as described in clause H.15.4.4.

H.15.5 Communication Forwarding unconditional / Fixed Broadband Access

H.15.5.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding unconditional. This process is described in 3GPP TS 24.604 [106].

H.15.5.2 Conformance requirement

As described in clause 15.5.2.

H.15.5.3 Test purpose

As described in clause 15.5.3.

H.15.5.4 Method of test

Initial conditions

UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN with xDSL, Fiber or Ethernet with SS. SS is configured with the HTTP Digest password for XCAP, related to the IMS private user identity (IMPI) configured on the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding unconditional, at step 7 deactivation of Communication Forwarding unconditional is respectively triggered at the UE.

H.15.5.5 Test requirements

As described in clause 15.5.5.

H.15.6 Communication Forwarding on non Reply: activation / Fixed Broadband Access

H.15.6.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user does not answer to the phone. This process is described in 3GPP TS 24.604 [106].

H.15.6.2 Conformance requirement

As described in clause 15.7.2.

H.15.6.3 Test purpose

As described in clause 15.7.3.

H.15.6.4 Method of test

Initial conditions

UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN with xDSL, Fiber or Ethernet with SS. SS is configured with the HTTP Digest password for XCAP, related to the IMS private user identity (IMPI) configured on the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding on non Reply, at step 7 deactivation of Communication Forwarding on non Reply is respectively triggered at the UE.

H.15.6.5 Test requirements

As described in clause 15.7.5.

H.15.7 Communication Forwarding on non reply: Originating call initiation / Fixed Broadband Access

H.15.7.1 Definition

Test to verify that the MTSI UE Originating correctly handles session setup where call is being forwarded due to no reply. This process is described in 3GPP TS 24.604 [106], clauses 4.2.1, 4.5.2.1 and A.1.3 and 3GPP TS 24.229 [10], clause 9.2.3

H.15.7.2 Conformance requirement

As described in clause 15.8.2.

H.15.7.3 Test purpose

As described in clause 15.8.3.

H.15.7.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration.

Test procedure

1-6) Steps 1-6, procedure C.21c.

7) SS responds to the INVITE with a valid 181 Call Is Being Forwarded response (simulate the UE to which call was forwarded)

8) SS responds to the INVITE request with 180 Ringing response.

9) As the 180 Ringing response was sent reliably, UE sends a PRACK request.

10) SS responds to PRACK with 200 OK.

11) SS responds to the INVITE request with a 200 OK response.

12) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

13) Call is released on the UE. SS waits the UE to send a BYE request.

14) SS responds to the BYE request with a 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-6			Steps 1-6 as defined in Annex C.21c	
7	←		181 Call is being forwarded	SS sends 181 response to indicate that call forwarding has been started as the user did not answer to the phone
8	←		180 Ringing	The SS sends 180 Ringing response to the UE
9	→		PRACK	UE acknowledges the receipt of 180 response by sending PRACK.
10	←		200 OK	The SS responds PRACK with 200 OK.
11	←		200 OK	The SS responds INVITE with 200 OK to indicate that the virtual remote UE had answered the call
12	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
13	→		BYE	The UE releases the call with BYE
14	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

181 Call is being forwarded (Step 7)

Use default message “181 Call is being forwarded” in annex A.2.14.

180 Ringing (Step 8)

Use the default message “180 Ringing for INVITE” in annex A.2.6 applying condition A3 (Response sent reliably) and with the following exceptions:

Header/param	Value/remark
To	
tag	different tag must be used than the one used in steps 3-7 as this response is now from another UE and belongs to another dialog instance. Note that this new tag must be used within the rest of the steps (8-14) in this test case.
Contact	
addr-spec	different URI must be used than the one used in step 3 as this is supposed now to represent another UE to which the call is being forwarded.. Note that this new Contact must be used within the rest of the steps (8-14) in this test case.
History-Info	
hi-targeted-to-uri	Same value as in the 181 response of step 7
hi-index	Same value as in the 181 response of step 7
Content-Type	
media-type	*application/sdp*
Message-body	Same contents as specified in step 4 annex C.21c. except for o-line: *o=- 22222222 22222222 IN* (addrtype) (unicast-address for new remote UE).

200 OK (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	Same value as in the 180 response of step 8
History-Info	
hi-targeted-to-uri	Same value as in the 181 response of step 7
hi-index	Same value as in the 181 response of step 7

H.15.7.5 Test requirements

The UE shall send requests and responses as described in clause H.15.7.4.

H.15.8 Communication Forwarding on Busy / Fixed Broadband Access

H.15.8.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is busy. This process is described in 3GPP TS 24.604 [106].

H.15.8.2 Conformance requirement

As described in clause 15.9.2.

H.15.8.3 Test purpose

As described in clause 15.9.3.

H.15.8.4 Method of test

Initial conditions

UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN with xDSL, Fiber or Ethernet with SS. SS is configured with the HTTP Digest password for XCAP, related to the IMS private user identity (IMPI) configured on the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding on Busy, at step 7 deactivation of Communication Forwarding on Busy is respectively triggered at the UE.

H.15.8.5 Test requirements

As described in clause 15.9.5.

H.15.9 Communication Forwarding on Not logged-in / Fixed Broadband Access

H.15.9.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is not registered to IMS service. This process is described in 3GPP TS 24.604 [106].

H.15.9.2 Conformance requirement

As described in clause 15.10.2.

H.15.9.3 Test purpose

As described in clause 15.10.3.

H.15.9.4 Method of test

Initial conditions

UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN with xDSL, Fiber or Ethernet with SS. SS is configured with the HTTP Digest password for XCAP, related to the IMS private user identity (IMPI) configured on the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding on Not logged-in, at step 7 deactivation of Communication Forwarding on Not logged-in is respectively triggered at the UE.

H.15.9.5 Test requirements

As described in clause 15.10.5.

H.15.10 Communication Forwarding on Not reachable / Fixed Broadband Access

H.15.10.1 Definition

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is not reachable. This process is described in 3GPP TS 24.604 [106].

H.15.10.2 Conformance requirement

As described in clause 15.10a.2.

H.15.10.3 Test purpose

As described in clause 15.10a.3.

H.15.10.4 Method of test

Initial conditions

UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated the IP-CAN with xDSL, Fiber or Ethernet with SS. SS is configured with the HTTP Digest password for XCAP, related to the IMS private user identity (IMPI) configured on the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Communication Forwarding on Not reachable, at step 7 deactivation of Communication Forwarding on Not reachable is respectively triggered at the UE.

H.15.10.5 Test requirements

As described in clause 15.10a.5.

H.15.11 Self-Configuration via SIP based procedure / Fixed Broadband Access

H.15.11.1 Definition

Test to verify that the UE correctly performs SIP-based user configuration. This process is described in 3GPP TS 24.238 [142].

H.15.11.2 Conformance requirement

[TS 24.238, clause 4.3.2]:

When performing SIP-based user configuration, the UE shall create a SIP URI, as described in RFC 4967 [4], with:

a) a dialstring, set to either the concatenation of feature code and the number to be provisioned or the feature code alone if no number information needs to be provided for the service; and

b) a "phone-context" parameter, set to the home network domain name.

The UE shall construct and initiate an appropriate INVITE in accordance with TS 24.229 [3] with the Request-URI set to the URI created above.

[TS 24.229, clause 5.1.2A.1]:

If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

When SIP digest is in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;
- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;
- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used); and

- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

[TS 24.229, clause 5.1.2A.1.2]:

The UE may use non-international formats of E.164 addresses, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

Local numbering information is sent in the Request-URI in initials requests or stand alone transaction, using one of the following formats:

1) a tel-URI, complying with RFC 3966, with a local number followed by a "phone-context" tel URI parameter value.

2) a SIP URI, complying with RFC 3261, with the "user" SIP URI parameter set to "phone".

3) a SIP URI, complying with RFC 3261 and RFC 4967, with the "user" SIP URI parameter set to "dialstring".

The actual value of the URI depends on whether user equipment performs an analysis of the dial string input by the end user or not.

[TS 24.229, clause 5.1.2A.1.5]:

When the UE uses home-local number, the UE shall include in the "phone-context" tel URI parameter the home domain name in accordance with RFC 3966.

When the UE uses geo-local number, the UE shall:

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header field into the request), include the access technology information in the "phone-context" tel URI parameter according to RFC 3966 as defined in clause 7.2A.10; and

- if access technology information is not available to the UE (i.e., the UE cannot insert P-Access-Network-Info header field into the request), include in the "phone-context" tel URI parameter the home domain name prefixed by the "geo-local" string according to RFC 3966 as defined in clause 7.2A.10.

When the UE uses other local numbers, than geo-local number or home local numbers , e.g. private numbers that are different from home-local number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966, e.g. if private numbers are used a domain name to which the private addressing plan is associated.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value inserted by the UE, based on implementation.

NOTE 2: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is implementation specific.

NOTE 3: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

[TS 24.229, clause 5.1.3.1]:

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and

- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

...

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it.

Reference(s)

TS 24.238[142], clause 4.3.2, TS 24.229[10], clause 5.1.2A.1, 5.1.2A.1.2, 5.1.2A.1.5, 5.1.3.1.

H.15.11.3 Test purpose

To verify that the UE can request activation of Communication Forwarding (unconditional) with a correctly composed INVITE request.

H.15.11.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE start SIP-based user configuration	
2	->		INVITE	UE sends INVITE with Request-URI set as “*21#”
3	<-		200 OK	SS responds INVITE with 200 OK
4	->		ACK	UE acknowledges
5	->		BYE	The UE releases the call with BYE
6	<-		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition "SIP Digest without TLS for Fixed Broadband Access" when applicable.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for Originating Call" in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Request-Line Method Request-URI	 INVITE “*21#”
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 6] - *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 7] - *a=rtpmap:* (payload type) *telephone-event* [Note 4] - *a=ecn-capable-rtp: leap ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=rtcp-rsize* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 3] - *a=crypto:1* *AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20|* *1:4FEC_ORDER=FEC_SRTP"* [Note 3] Note 1: At least one "c=" field shall be present. Note 2: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: a rate may be added to the “telephone-event” separated by “/” (e.g. “telephone-event/8000”) Note 5: The RR value must be greater than 0. The RS value can be any value. Note 6: The AMR channel number shall be “/1” or omitted. Note 7: values from 0 to 220 are allowed

H.15.11.5 Test requirements

The UE shall send requests and responses as described in clause H.15.11.4.

H.16 Void

H.17 Media use cases

H.17.1 Originating Voice, add video remove video / Fixed Broadband Access

H.17.1.1 Definition

Test to verify that the UE is able to add a bidirectional video component to an ongoing UE Originating IMS Multimedia telephony voice call for Fixed Broadband Access. This process is described in TS 24.229 [10], TS 24.173 [65] and TS 26.114 [66].

H.17.1.2 Conformance requirement

Same as described in 17.1.2.

H.17.1.3 Test purpose

1) To verify that when adding a video component to an ongoing IMS Multimedia Telephony voice call the UE performs correct exchange of SIP protocol signalling messages; and

2) To verify that within SIP signalling the UE performs correct SDP offer/answer exchanges for negotiating media and indicating preconditions for resource reservation (as described by TS 24.229 [10], clause 6.1); and

3) To verify that when removing the video component from the IMS Multimedia Telephony call the UE performs correct exchange of SIP and SDP protocol messages.

H.17.1.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration. SS has also performed the Originating voice Call according to C.21c.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt add IMS video to the voice call.	
2	->		INVITE	UE sends re-INVITE with a SDP offer containing media lines for both voice and video
3	<-		100 Trying	SS sends a 100 Trying provisional response
4-6				Void
7	<-		200 OK	SS responds INVITE with 200 OK
8	->		ACK	UE acknowledges
9			Make UE release video from media call	
10	->		INVITE	UE sends re-INVITE with a SDP offer indicating that the video component is removed from the call
11	<-		100 Trying	The SS responds with a 100 Trying provisional response
12	<-		200 OK	The SS responds re-INVITE with 200 OK
13	->		ACK	The UE acknowledges the receipt of 200 OK for re-INVITE
14	->		BYE	The UE releases the call with BYE
15	<-		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition "SIP Digest without TLS for Fixed Broadband Access" when applicable.

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in clause A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=*(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 6] - *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 7] - *a=fmtp:* (format) - *a=ptime:20* - *a=maxptime:240* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 8] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 8] - *a=pcfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id=* (att-field) Note 1: At least one "c=" field shall be present. Note 2: Void. Note 3: Void. Note 4: a rate may be added to the “telephone-event” separated by “/” (e.g. “telephone-event/8000”) Note 5: Void. Note 6: The AMR channel number shall be “/1” or omitted. Note 7: values from 0 to 220 are allowed Note 8: The tcap/pcfg attributes are present if RTP/AVP is present on the m line.

200 OK (Step 7)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/Remark
Content-Type **media-type**	 *application/sdp*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:* bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000/1* [Note 1] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* [Note 1] - *a=ptime:20* - *a=maxptime:240* Media description: - *m=video* (transport port) *RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a= acfg:1 t=1* [Note 2] - *a=rtpmap:* (payload type) *H264/90000* - *a=fmtp:* (format) *profile-level-id*= (att-field) Note 1: The value for fmt, bandwidth, payload type and format specific parameters copied from step 2. Note 2: Present if tcap/pcfg attributes were included in step 2. Note 3: Void. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: Void.

INVITE (Step 10)

Use the default message "INVITE for MO Call" in clause A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 6] - *a=fmtp:* (format) - *a=ptime:20* - *a=maxptime:240* Media description: - *m=video 0 RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Note 1: At least one "c=" field shall be present. Note 2: Void. Note 3: Void. Note 4: Void Note 5: Void. Note 6: The AMR channel number shall be “/1” or omitted. Note 7: Void.

200 OK (Step 12)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Content-Length	
Value	length of message-body
Message-body	SDP body of the 200 response copied from the received INVITE and modified as follows: - "o=" line identical to previous SDP sent by SS except that sess-version is incremented by one - IP address on "c=" line and, for audio, transport port on "m=" line changed to indicate to which IP address and port the UE should start sending the media;

H.17.1.5 Test requirements

The UE shall send requests and responses as described in clause H.17.1.4

H.17.2 Terminating Voice, add video remove video / Fixed Broadband Access

H.17.2.1 Definition

Test to verify that the UE is able to add a bidirectional video component to an ongoing UE terminating IMS Multimedia telephony voice call for Fixed Broadband Access. This process is described in TS 24.229 [10], TS 24.173 [65] and TS 26.114 [66].

H.17.2.2 Conformance requirement

Same as described in clause 17.2.2.

H.17.2.3 Test purpose

1) To verify that when adding a video component to an ongoing IMS Multimedia Telephony voice call the UE performs correct exchange of SIP protocol signalling messages; and

2) To verify that within SIP signalling the UE performs correct SDP offer/answer exchanges for negotiating media and indicating preconditions for resource reservation (as described by TS 24.229 [10], clause 6.1); and

3) To verify that when removing the video component from the IMS Multimedia Telephony call the UE performs correct exchange of SIP and SDP protocol messages.

H.17.2.4 Method of test

Initial conditions

UE is configured with the home domain name, public and private user identities and SIP Digest Credentials.

SS is configured with the home domain name, public and private user identities and SIP Digest Credentials. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform MD5 authentication algorithm for that IMPI, according to TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS has performed MD5 authentication with the UE and accepted the registration. SS has also performed the UE Terminating voice Call according to C.11c.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends re-INVITE with second SDP offer to add video.
2	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
3-5				Void
6				Make UE accept the speech and video offer. (this is done either after receiption of 100 Trying or after 5s)
7	→		200 OK	The UE responds to the re-INVITE with a 200 OK final response.
8	←		ACK	The SS acknowledges the receipt of 200 OK for the re-INVITE.
9	←		INVITE	SS sends a re-INVITE with a SDP offer indicating that the video component is removed from the call.
10	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
11	→		200 OK	The UE responds to the re-INVITE with a 200 OK final response.
12	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
13	←		BYE	The SS sends BYE to release the call.
14	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition "SIP Digest without TLS for Fixed Broadband Access" when applicable.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in clause A.2.9 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS: 352* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Media description: *- m=video (transport port) RTP/AVPF 101* *- b=AS: 315* *- b=RS: 0* *- b=RR: 2500* Attributes for media: *- a=rtpmap:101 H264/90000* *- a=fmtp: 101 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* *- a=rtcp-fb:* trr-int 5000* *- a=rtcp-fb:* nack* *- a=rtcp-fb:* nack pli* *- a=rtcp-fb:* ccm fir* *- a=rtcp-fb:* ccm tmmbr*

200 OK (Step 7)

Use the default message “200 OK for other requests than REGISTER or SUBSCRIBE” in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Message-body	The following SDP types and values shall be present. [Note 3] Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2] Media description: - *m=video (transport port) RTP/AVPF* (fmt) [Note 2] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *H264/90000* [Note 2] - *a=fmtp:* (format) *packetization-mode=0;profile-level-id=(att-field); * Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked Note 3: Parameters for the AMR codec are not checked

INVITE (Step 9)

Use the default message "INVITE for MT Call" in clause A.2.9 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99* - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Media description: *- m=video (transport port) RTP/AVPF 101* *- b=AS: 315* *- b=RS: 0* *- b=RR: 2500* Attributes for media: *- a=rtpmap: 101 H264/90000* *- a=fmtp:* 101*packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* *- a=rtcp-fb:* trr-int 5000* *- a=rtcp-fb:* nack* *- a=rtcp-fb:* nack pli* *- a=rtcp-fb:* ccm fir* *- a=rtcp-fb:* ccm tmmbr*

200 OK (Step 12)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in clause A.3.1 with the following exceptions when there is no SDP in 180 Ringing.

Header/param	Value/remark
Require option-tag	 *precondition*
Content-Type media-type	 *application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body length of message-body
Message-body	SDP body not checked.

H.17.2.5 Test requirements

The UE shall send requests and responses as described in clause H.17.2.4

Annex I (normative): IMS for Converged IP Communications

I.1 Scope

The present annex defines test cases dedicated to IMS for Converged IP Communications, i.e., the provision of multi-media telephony, exercising scenarios described in GSMA PRD NG.102 [144].

Within this Annex, the UE is assumed to attach via an E-UTRAN or EPC-integrated WLAN access network.

As described in section 1.1 of GSMA PRD NG.102 [144], the following network deployments are supported:

- a converged IMS core network (i.e. supporting all Converged IP Communications Services), or
- two separate IMS core networks (i.e. one IMS core network supporting Multimedia Telephony and SMSoIP and another IMS core network supporting all other advanced messaging services excluding both Multimedia Telephony and SMSoIP).

The network deployments described above require that the UE supports:

- a single IMS registration to a single IMS core network; and
    - two separate IMS registrations, either to a single IMS core network or to two separate IMS core networks.

I.2 to I.7 Void

I.8 Registration / Converged IP Communications

I.8.1 Initial registration / Converged IP Communications

I.8.1a Single IMS Registration via E-UTRA / Converged IP Communications

I.8.1a.1 Definition

Test to verify that the UE can correctly register to IMS for Converged IP Communications [144] via E-UTRA when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing to the registration event package for the registered default public user identity, using E-UTRA access. The single registration shall register multi-media telephony, SMSoIP and advanced messaging services via a single IMS core network.

I.8.1a.2 Conformance requirement

As described in clause 8.1.2. In addition,

a) to verify that the UE performs a single IMS registration for multi-media telephony, SMSoIP and advanced messaging services using the IMS APN over E-UTRA access.

I.8.1a.3 Test purpose

As described in clause 8.1.3. In addition:

a) to verify that the UE performs a single IMS registration for multi-media telephony, SMSoIP and advanced messaging services using the IMS APN over E-UTRAN access.

I.8.1a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is capable of Converged IP Communications [144], and the UE determined that one APN is to be used for SIP signalling as configuration parameter “RCS VOLTE SINGLE REGISTRATION is set to 1, configuration parameter “NO MSRP SUPPORT” is set to empty value, and UE is not roaming outside its HPMN.

Test procedure

UE executes the procedures described in TS 36.508 [94] subclause 4.5.2.3.

SS checks that the UE does not send a second REGISTER request after completing procedure C.2.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-11			Steps 1-11 defined in Annex C.2	
12				The SS waits 10 seconds in order to check that the UE does not send another REGISTER request.

I.8.1a.5 Test requirements

The UE shall send requests and responses as described in clause I.8.1a.4.

I.8.1b Dual IMS Registration via E-UTRA / Converged IP Communications

I.8.1b.1 Definition

Test to verify that the UE can correctly register to IMS for Converged IP Communications [144] via E-UTRA when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending two IMS registrations, each to the respective S-CSCF via the respective P-CSCF discovered, authenticating the user and finally subscribing to the registration event package for the registered default public user identity, using E-UTRA access (authentication and subscription happens once per registration). One IMS registration shall register multi-media telephony and SMSoIP, and the second registration shall register advanced messaging services.

I.8.1b.2 Conformance requirement

For the registration for multi-media telephony and SMSoIP, as described in clause I.8.1a.2.

I.8.1b.3 Test purpose

As described in clause 8.1.3. In addition:

a) to verify that the UE performs two IMS registrations, one for multi-media telephony and SMSoIP using the IMS APN, and another one for advanced messaging services using the HOS APN, both over E-UTRAN access.

I.8.1b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is capable of Converged IP Communications [144], and the UE determined that two APN's are to be used for SIP signalling as configuration parameter "RCS VOLTE SINGLE REGISTRATION is set to 0, configuration parameter "NO MSRP SUPPORT" is set to empty value, and UE is not roaming outside its HPMN.

Test procedure

UE executes the procedures described in TS 36.508 [94] table 4.5A.28.3-1.

I.8.1b.5 Test requirements

The UE shall send requests and responses as described in clause I.8.1b.4.

I.8.1c Single IMS Registration via WLAN / Converged IP Communications

I.8.1c.1 Definition

Test to verify that the UE can correctly register to IMS for Converged IP Communications [144] via EPC-integrated WLAN when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing to the registration event package for the registered default public user identity, using WLAN access. The single registration shall register multi-media telephony, SMSoIP and advanced messaging services via a single IMS core network.

I.8.1c.2 Conformance requirement

As clause I.8.1a.2.

I.8.1c.3 Test purpose

As described in clause G.8.1.3. In addition,

a) to verify that the UE performs a single IMS registration for multi-media telephony, SMSoIP and advanced messaging services using the IMS APN over integrated WLAN access.

I.8.1c.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is capable of Converged IP Communications [144], and the UE determined that one APN is to be used for SIP signalling as configuration parameter "RCS VOLTE SINGLE REGISTRATION is set to 1, configuration parameter "NO MSRP SUPPORT" is set to empty value, and UE is not roaming outside its HPMN.

Test procedure

As described in C.2c using WLAN access.

SS checks that the UE does not send a second REGISTER request after completing above procedure.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-9				Steps 1-9 of Annex C.2c
10				The SS waits 10 seconds in order to check that the UE does not send another REGISTER request.

I.8.1c.5 Test requirements

The UE shall send requests and responses as described in clause I.8.1c.4.

I.8.1d Dual Registration via WLAN / Converged IP Communications

I.8.1d.1 Definition

Test to verify that the UE can correctly register to IMS for Converged IP Communications [144] via EPC-integrated WLAN when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending two IMS registrations, each to the respective S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing the registration event package for the registered default public user identity, using integrated WLAN access (authentication and subscription happens once per registration). One IMS registration shall register multi-media telephony and SMSoIP, and the second registration shall register advanced messaging services.

I.8.1d.2 Conformance requirement

As clause I.8.1b.2.

I.8.1d.3 Test purpose

As described in clause G.8.1.3. In addition:

a) to verify that the UE performs two IMS registrations, one for multi-media telephony and SMSoIP using the IMS APN, and another one for advanced messaging services using the HOS APN, over integrated WLAN access.

I.8.1d.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is capable of Converged IP Communications [144], and the UE determined that two APN's are to be used for SIP signalling as configuration parameter "RCS VOLTE SINGLE REGISTRATION is set to 0, configuration parameter "NO MSRP SUPPORT" is set to empty value, and UE is not roaming outside its HPMN.

Test procedure

As described in C.2c using WLAN access.

In order to establish a second IPsec tunnel, the UE executes the procedures described in TS 36.508 [94] table 4.5A.29.3-1. Then, the UE executes steps 2-9 of C.2c.

I.8.1d.5 Test requirements

The UE shall send requests and responses as described in clause I.8.1d.4.

I.9 to I.11 Void

I.12 Call Control / Converged IP Communications

I.12.1a MO voice call / single / E-UTRA

I.12.1a.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup and release over E-UTRA after having registered Multimedia Telephony and SMSoIP services as well as other RCS services using the IMS well-known APN.

I.12.1a.2 Conformance requirement

As described in clause 12.12.2.

I.12.1a.3 Test purpose

As described in clause 12.12.3. In addition:

a) to verify that the UE uses the IMS APN for initiating the voice call over E-UTRA after having registered Multimedia Telephony and SMSoIP services as well as other RCS services using the IMS well-known APN.

I.12.1a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the test procedure in clause I.8.1a.4 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

As described in clause 12.12.4

I.12.1a.5 Test requirements

The UE shall send requests and responses as described in clause I.12.1a.4.

I.12.1b MO voice call / dual / E-UTRA

I.12.1b.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup and release over E-UTRA after having registered Multimedia Telephony and SMSoIP services using the IMS well-known APN, and other RCS services using the HOS APN.

I.12.1b.2 Conformance requirement

As described in clause 12.12.2.

I12.1b.3 Test purpose

As described in clause 12.12.3. In addition:

a) to verify that the UE uses the IMS APN for initiating the voice call over E-UTRA while other RCS services where registered to use the HOS APN.

I.12.1b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC.

UE is capable of Converged IP Communications [141], and the UE determined that two APNs are to be used for SIP signalling as configuration parameter “RCS VOLTE SINGLE REGISTRATION is set to 0, configuration parameter “NO MSRP SUPPORT” is set to empty value, and UE is not roaming outside its HPMN.

UE has discovered two P-CSCFs and performed two IMS registrations, one for multi-media telephony and SMSoIP using the IMS APN, and another one for advanced messaging services using the HOS APN, over E-UTRAN access by executing the generic test procedure in clause I.8.1b.4 up to the last step.

Test procedure

MO voice call is set up, as described in clause 12.12 whereby the voice call is performed using the IMS well-known APN for SIP signalling and media.

I.12.1b.5 Test requirements

The UE shall send requests and responses as described in clause I.12.1b.4.

I.12.1c MO voice call / single / WLAN

I.12.1c.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup and release over WLAN after having registered Multimedia Telephony and SMSoIP services as well as other RCS services using the IMS well-known APN.

I.12.1c.2 Conformance requirement

As described in clause 12.12.2.

I.12.1c.3 Test purpose

As described in clause 12.12.3. In addition:

a) to verify that the UE uses the IMS APN for initiating the voice call over WLAN after having registered Multimedia Telephony and SMSoIP services as well as other RCS services using the IMS well-known APN.

I.12.1c.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered Multimedia Telephony and SMSoIP services as well as RCS services over WLAN by executing the test procedure in clause I.8.1c.4 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure

As described in clause G.8.1.4

I.12.1c.5 Test requirements

The UE shall send requests and responses as described in clause I.12.1c.4.

I.12.1d MO voice call / dual / WLAN

I.12.1d.1 Definition

Test to verify that the UE correctly performs IMS mobile originated voice call setup and release over WLAN after having registered Multimedia Telephony and SMSoIP services using the IMS well-known APN, and other RCS services using the HOS APN.

I.12.1d.2 Conformance requirement

As described in clause 12.12.2.

I.12.1d.3 Test purpose

As described in clause 12.12.3. In addition:

a) to verify that the UE uses the IMS APN for initiating the voice call over E-UTRA while other RCS services where registered to use the HOS APN.

I.12.1d.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC.

UE is capable of Converged IP Communications [141], and the UE determined that two APNs are to be used for SIP signalling as configuration parameter "RCS VOLTE SINGLE REGISTRATION is set to 0, configuration parameter "NO MSRP SUPPORT" is set to empty value, and UE is not roaming outside its HPMN.

UE has discovered two P-CSCFs and performed two IMS registrations, one for multi-media telephony and SMSoIP using the IMS APN, and another one for advanced messaging services using the HOS APN, over E-UTRAN access by executing the generic test procedure in clause I.8.1d.4 up to the last step.

Test procedure

As described in clause G.12.1.4 whereby the voice call is performed using the IMS well-known APN for SIP signalling and media.

I.12.1d.5 Test requirements

The UE shall send requests and responses as described in clause I.12.1d.4.

I.12.2a RCS chat / single / E-UTRA

I.12.2a.1 Definition

Test to verify that the UE correctly starts initiating a 1-1 chat session over E-UTRA after having registered Multimedia Telephony and SMSoIP services as well as other RCS services using the IMS well-known APN.

I.12.2a.2 Conformance requirement

n/a

I.12.2a.3 Test purpose

Verify that the UE uses the IMS well-known APN to initiate a 1-1 chat session over E-UTRA, using the IMS well-known APN.

I.12.2a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the test procedure in clause I.8.1a.4 up to the last step.

Test procedure

1) UE sends INVITE as described in Annex A.2.1 with conditions A1 and A4

2) SS responds by sending 503 Service Unavailable as described in annex A.4.2

3) UE sends ACK as described in Annex A.2.7 with condition A4 "ACK for non-2xx response"

I.12.2a.5 Test requirements

UE must run initiation of the chat session using the IMS well-known APN, over which it first registered Multimedia Telephony and SMSoIP services as well as other RCS services

The UE shall send requests and responses as described in clause I.12.2a.4.

I.12.2b RCS chat / dual / E-UTRA

I.12.2b.1 Definition

Test to verify that the UE correctly starts initiating a 1-1 chat session over E-UTRA after having registered Multimedia Telephony and SMSoIP services using the IMS well-known APN, and other RCS services using the HOS APN.

I.12.2b.2 Conformance requirement

n/a

I12.2b.3 Test purpose

Verify that the UE uses the HOS APN to initiate a 1-1 chat session over E-UTRA.

I.12.2b.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the test procedure in clause I.8.1b.4 up to the last step.

Test procedure

1) UE sends INVITE as described in Annex A.2.1 with conditions A1 and A4, using the HOS APN.

2) SS responds by sending 503 Service Unavailable as described in annex A.4.2.

3) UE sends ACK as described in Annex A.2.7 with condition A4 “ACK for non-2xx response”.

I.12.2b.5 Test requirements

UE must run initiation of the chat session using the HOS APN, over which it had registered RCS services.

The UE shall send requests and responses as described in clause I.12.2b.4.

I.12.2c RCS chat / single / WLAN

I.12.2c.1 Definition

Test to verify that the UE correctly starts initiating a 1-1 chat session over WLAN after having registered Multimedia Telephony and SMSoIP services as well as other RCS services using the IMS well-known APN.

I.12.2c.2 Conformance requirement

n/a

I12.2c.3 Test purpose

Verify that the UE uses the IMS well-known APN to initiate a 1-1 chat session over WLAN.

I.12.2c.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the test procedure in clause I.8.1c.4 up to the last step.

Test procedure

1) UE sends INVITE as described in Annex A.2.1 with conditions A1 and A4
2) SS responds by sending 503 Service Unavailable as described in annex A.4.2
3) UE sends ACK as described in Annex A.2.7 with condition A4 “ACK for non-2xx response”

I.12.2c.5 Test requirements

The UE shall send requests and responses as described in clause I.12.2c.4.

I.12.2d RCS chat / dual / WLAN

I.12.2d.1 Definition

Test to verify that the UE correctly starts initiating a 1-1 chat session over E-UTRA after having registered Multimedia Telephony and SMSoIP services using the IMS well-known APN, and other RCS services using the HOS APN.

I.12.2d.2 Conformance requirement

n/a

I12.2d.3 Test purpose

Verify that the UE uses the HOS APN to initiate a 1-1 chat session over WLAN.

I.12.2d.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the test procedure in clause I.8.1d.4 up to the last step.

Test procedure

1) UE sends INVITE as described in Annex A.2.1 with conditions A1 and A4, using the HOS APN.
2) SS responds by sending 503 Service Unavailable as described in annex A.4.2.
3) UE sends ACK as described in Annex A.2.7 with condition A4 “ACK for non-2xx response”.

I.12.2d.5 Test requirements

The UE shall send requests and responses as described in clause I.12.2d.4.

Annex J (normative): IP-Connectivity Access Network specific test cases for category M1 UEs when accessing the IM CN subsystem

J.1 Scope

The present annex defines IP-CAN specific test cases for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is Evolved Packet System (EPS). The EPS core network use an E-UTRAN radio access network. The UE is a category M1 and adheres to GSMA profile NG.108 [151].

J.2 to J.7

J.8 Registration / UE category M1

J.8.1 Initial registration / UE category M1

J.8.1.1 Definition

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing the registration event package for the registered default public user identity on a category M1 UE.

J.8.1.2 Conformance requirement

As described in clause 8.1.2.

J.8.1.3 Test purpose

As described in clause 8.1.3

J.8.1.4 Method of test

As described in generic procedure C.2.

J.8.1.5 Test requirements

As described in clause 8.1.5

J.9 to J.11

J.12 Call Control

J.12.1 MO MTSI speech call / UE category M1

J.12.1.1 Definition

Test to verify that the UE correctly setup a IMS mobile originated speech call on a category M1 UE and release it. This process is described in 3GPP TS 24.229 [10], clauses 5.1.2A.1, 5.1.3 and 6.1, and TS 26.114 [66], clauses 5.2.1, 6.2.2.1, 6.2.5 and 7.3.1.

J.12.1.2 Conformance requirement

As described in clause 12.12.2.

J.12.1.3 Test purpose

As described in clause 12.12.3.

J.12.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a category M1 UE (TS 34.229-2 [5] A.18/1 and TS 36.523-2 [147] A.4.3.2-2A/1)

1-14) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to14.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.21d	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
14			The UE is triggered by MMI to release the call	
15	→		BYE	The UE releases the call with BYE
16	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Steps 1 - 13 as specified in annex C.21d

J.12.1.5 Test requirements

The UE shall send requests and responses as described in clause J.12.1.4.

J.12.2 MT MTSI speech call / UE category M1

J.12.2.1 Definition

Test to verify that the UE correctly setup a IMS mobile terminated speech call on a category M1 UE and release it. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66].

J.12.2.2 Conformance requirement

As described in clause 12.13.2.

J.12.2.3 Test purpose

As described in clause 12.13.3.

J.12.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1 and TS 36.523-2 [147] A.4.3.2-2A/1)

1 - 26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to 26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.11d	MTSI MT speech call. Referred from 36.508 [94] table 4.5A.7.3-1 for a UE with E-UTRA support.

Specific Message Contents

Steps 1 - 15 as specified in annex C.11d

J.12.2.5 Test requirements

The UE shall send requests and responses as described in clause J.12.2.4.

J.13 to J.14

J.15 Supplementary Services

J.15.1 Communication Waiting and answering the call / UE category M1

J.15.1.1 Definition

Test to verify that the MT UE correctly performs MTSI Communication Waiting. This process is described in 3GPP TS 24.615 [95].

J.15.1.2 Conformance requirement

As described in clause 15.27.2.

J.15.1.3 Test purpose

As described in clause 15.27.3.

J.15.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) with SS. The UE has registered to IMS and set up the MO call according the procedures C.2 and C.21d, as described in TS 36.508 [94] table 4.5A.6.3-1,

Test procedure applicable for a category M1 UE (TS 34.229-2 [5] A.18/1 and TS 36.523-2 [147] A.4.3.2-2A/1)

As described in clause 15.27.4, steps 1-15. Except, steps 1-8 replaced by steps in C.11d.

J.15.1.5 Test requirements

As described in clause 15.27.5.

J.15.2 Communication Waiting and cancelling the call / UE category M1

J.15.2.1 Definition

Test to verify that the UE correctly performs IMS Multimedia Telephony Communication Waiting (CW) terminal based procedure. This process is described in 3GPP TS 24.615 [95].

J.15.2.2 Conformance requirement

As described in clause 15.28.2.

J.15.2.3 Test purpose

As described in clause 15.28.3.

J.15.2.4 Method of test

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) with SS. The UE has registered to IMS and set up the MO call according the procedures C.2 and C.21d, as described in TS 36.508 [94] table 4.5A.6.3-1,

Test procedure applicable for a category M1 UE (TS 34.229-2 [5] A.18/1 and TS 36.523-2 [147] A.4.3.2-2A/1)

As described in clause 15.28.4, steps 1-15. Except, steps 1-8 replaced by steps in C.11d.

J.15.2.5 Test requirements

As described in clause 15.28.5.

J.15.3 Subscription to the MWI event package / UE category M1

J.15.3.1 Definition

Test to verify that the UE is able to subscribe to MTSI message waiting notification and handle such notifications received after subscription. This process is described in 3GPP TS 24.229 [10] and TS 24.606 [107].

J.15.3.2 Conformance requirement

As described in clause 15.15.2.

J.15.3.3 Test purpose

As described in clause 15.15.3.

J.15.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) with SS. The UE has registered to IMS according the procedure C.2 steps 1 to 7.

The UE is pre-configured to autonomously subscribe to the Message Waiting Indication package. The UE is configured with the public service identity of the message account. Otherwise the phone is expected to use the public identity of the user when subscribing to the Message Waiting Indication package.

Test procedure

As described in clause 15.15.4.

J.15.3.5 Test requirements

As described in clause 15.15.5.

J.15.4 Originating Identification Restriction / UE category M1

J.15.4.1 Definition

Test to verify that the UE correctly invokes the IMS Multimedia Telephony Originating Identification Restriction. This process is described in 3GPP TS 24.607 [102].

J.15.4.2 Conformance requirement

As described in clause 15.2a.2.

J.15.4.3 Test purpose

As described in clause 15.2a.3.

J.15.4.4 Method of test

Initial conditions

Same as clause J.12.1 with the following addition:

The UE is configured for Originating Identification Restriction

Test procedure

As described in clause 15.2a.4, steps 1-14. Except, steps 2-13 replaced by steps in C.21d.

J.15.4.5 Test requirements

As described in clause 15.2a.5.

J.15.5 Terminating Identification Restriction / UE category M1

J.15.5.1 Definition

Test to verify that the UE correctly invokes the IMS Multimedia Telephony Terminating Identification Restriction. This process is described in 3GPP TS 24.608 [103].

J.15.5.2 Conformance requirement

As described in clause 15.4a.2.

J.15.5.3 Test purpose

As described in clause 15.4a.3.

J.15.5.4 Method of test

Initial conditions

Same as clause J.12.2 with the following addition:

The UE is configured for Terminating Identification Restriction

Test procedure

As described in clause 15.4a.4, steps 1-16. Except, steps 1-11 and 13-16 replaced by steps in C.11d.

J.15.5.5 Test requirements

As described in clause 15.4a.5.

J.15.6 Communication forwarding on non reply: MO call initiation / UE category M1

J.15.6.1 Definition

Test to verify that the MTSI MO UE correctly handles session setup where call is being forwarded due to no reply. This process is described in 3GPP TS 24.604 [106], clauses 4.2.1, 4.5.2.1 and A.1.3 and 3GPP TS 24.229 [10], clause 9.2.3

J.15.6.2 Conformance requirement

As described in clause 15.8.2.

J.15.6.3 Test purpose

As described in clause 15.8.3.

J.15.6.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated the IP-CAN to the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN) with SS. The UE has registered to IMS according the procedure C.2.

Test procedure applicable for a category M1 UE (TS 34.229-2 [5] A.18/1 and TS 36.523-2 [147] A.4.3.2-2A/1)

As described in clause 15.8.4, steps 1-18. Except, steps 1-9B and 12-13B replaced by steps in C.21d, and that step 11 uses AMR instead of AMR-WB codec.

J.15.6.5 Test requirements

The UE shall send requests and responses as described in clause J.15.6.4.

J.16 to J.17

J.18 SMS over IMS / UE category M1

J.18.1 Mobile Originating SMS / UE category M1

J.18.1.1 Definition

Test to verify that the UE is able to send a Mobile Originating SMS over IMS and to receive a status report.

J.18.1.2 Conformance requirement

As described in clause 18.1.2

J.18.1.3 Test purpose

As described in clause 18.1.3

J.18.1.4 Method of test

As described in clause 18.1.4

J.18.1.5 Test requirements

As described in clause 18.1.5

J.18.2 Mobile Terminating SMS / UE category M1

J.18.2.1 Definition

Test to verify that the UE correctly implemented the role of an SM-over-IP receiver.

J.18.2.2 Conformance requirement

As described in clause 18.2.2

J.18.2.3 Test purpose

As described in clause 18.2.3

J.18.2.4 Method of test

As described in clause 18.2.4

J.18.2.5 Test requirements

As described in clause 18.2.5

J.19 Emergency Service over IMS

J.19.1 Emergency call with emergency registration / Success / Location information available / UE category M1

J.19.1.1 Definition

As described in clause 19.1.1.1.

J.19.1.2 Conformance requirement

As described in clause 19.1.1.2.

J.19.1.3 Test purpose

As described in clause 19.1.1.3.

J.19.1.4 Method of test

Initial conditions

As described in clause 19.1.1.4.

Test procedure applicable for a category M1 UE (TS 34.229-2 [5] A.18/1 and TS 36.523-2 [147] A.4.3.2-2A/1)

As described in clause 19.1.1.4.

J.19.1.5 Test requirements

As described in clause 19.1.1.5.

J.19.2 Emergency call with emergency registration / Success / Location information not available / UE category M1

J.19.2.1 Definition

As described in clause 19.1.2.1.

J.19.2.2 Conformance requirement

As described in clause 19.1.2.2.

J.19.2.3 Test purpose

As described in clause 19.1.2.3.

J.19.2.4 Method of test

Initial conditions

As described in clause 19.1.2.4.

Test procedure applicable for a category M1 UE (TS 34.229-2 [5] A.18/1 and TS 36.523-2 [147] A.4.3.2-2A/1)

As described in clause 19.1.2.4.

J.19.2.5 Test requirements

As described in clause 19.1.2.5.

Annex K (normative): Void

Annex L (informative): Change history

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-31	RP-060052	-	-	Update to version 1.0.0 and present to RAN#31 for information	-	0.0.1	1.0.0	R5-060292
-	-	-	-	Update to version 2.0.0 at RAN5#31	-	1.0.0	2.0.0	R5-061398
-	-	-	-	Update to version 2.1.0 during RAN5#31 e-mail agreement procedure	-	2.0.0	2.1.0	R5-061398r1
RP-32	RP-060269	-	-	MCC Editorial clean up version 2.1.1 - and present to RAN#32 for approval to go under revision control (as version 5.0.0)	-	2.1.0	2.1.1	-
-	-	-	-	Update to version 5.0.0 after RAN#32	-	2.1.1	5.0.0	-
RP-33	RP-060565	0001	-	Correction to TS 34.229-1 contents	F	5.0.0	5.1.0	R5-062360
RP-33	RP-060565	0002	-	Clarification to Emergency Test Case	F	5.0.0	5.1.0	R5-062543
RP-33	RP-060565	0003	-	Clarifications for SDP handling in TC 12.1 MO Call Successful	F	5.0.0	5.1.0	R5-062309
RP-33	RP-060565	0004	-	Test Case Correction on SigComp in the Initial registration	F	5.0.0	5.1.0	R5-062362
RP-33	RP-060565	0005	-	New TC on SigComp in the MO Call	F	5.0.0	5.1.0	R5-062323
RP-33	RP-060565	0006	-	Correction to authentication test case 9.2 Invalid Behaviour – SQN out of range	F	5.0.0	5.1.0	R5-062372
RP-33	RP-060565	0007	-	New TC on SigComp in the MT Call	F	5.0.0	5.1.0	R5-062363
RP-33	RP-060565	0008	-	New test cases for P-CSCF Discovery List	F	5.0.0	5.1.0	R5-062364
RP-33	RP-060565	0009	-	General IMS testing corrections and clarifications	F	5.0.0	5.1.0	R5-062371
RP-33	RP-060565	0010	-	Alignment with TS 24.229 version 5.16.0 affecting TCs 8.1, 8.2, 8.3 and the default message REGISTER.	F	5.0.0	5.1.0	R5-062215
RP-33	RP-060565	0011	-	Correction for TC 8.4: Invalid Behaviour – 423 Interval Too Brief	F	5.0.0	5.1.0	R5-062216
RP-33	RP-060565	0012	-	Correction for TCs 9.1and 9.2	F	5.0.0	5.1.0	R5-062370
RP-34	RP-060746	0013	-	Introduction of default messages and generic registration test procedure for early IMS security	F	5.1.0	5.2.0	R5-063332
RP-34	RP-060746	0014	-	Introduction of a registration test case for early IMS security	F	5.1.0	5.2.0	R5-063384
RP-34	RP-060746	0015	-	Updating of test cases to cover both IMS support and early IMS security scenarios	F	5.1.0	5.2.0	R5-063529
RP-34	RP-060746	0016	-	Introduction of a registration test case for combined IMS support and early IMS security	F	5.1.0	5.2.0	R5-063526
RP-34	RP-060746	0017	-	Introduction of a registration test case for combined IMS support and early IMS security and UICC with SIM application	F	5.1.0	5.2.0	R5-063385
RP-34	RP-060746	0018	-	Removal of MO Call - 488 not accepted here for Rel 5	F	5.1.0	5.2.0	R5-063330
RP-34	RP-060746	0019	-	Clarifications to MT test case	F	5.1.0	5.2.0	R5-063386
RP-34	RP-060746	0020	-	Corrections to MO with sigcomp test case	F	5.1.0	5.2.0	R5-063387
RP-34	RP-060746	0021	-	Corrections to P-CSCF Discovery (IPv6) test cases	F	5.1.0	5.2.0	R5-063388
RP-34	RP-060746	0022	-	New TCs on SigComp Invalid Behaviour	F	5.1.0	5.2.0	R5-063389
RP-34	RP-060746	0023	-	Addition of annex with the test ISIM parameters	F	5.1.0	5.2.0	R5-063390
RP-34	RP-060746	0024	-	Introduction of a postamble for IMS testing	F	5.1.0	5.2.0	R5-063391
RP-34	RP-060746	0025	-	Correction to Generic DHCP test procedure	F	5.1.0	5.2.0	R5-063242
RP-34	RP-060746	0027	-	Clarifications for IMS emergency call test case 14.2	F	5.1.0	5.2.0	R5-063522
RP-34	RP-060746	0028	-	Clarification of Default Message for IMS emergency call test case 14.2	F	5.1.0	5.2.0	R5-063523
RP-34	RP-060748	0033	-	Update of PDP Context and P-CSCF Discovery test cases to Rel-6	F	5.1.0	5.2.0	R5-063572
RP-34	RP-060746	0026	-	Production of pointer version 5.2.0 of TS 34.229-1 with no technical contents	F	5.1.0	5.2.0	R5-063291
RP-34	RP-060748	0029	-	Updates to TC 11.1 Network-initiated deregistration for IMS Rel-6	F	5.1.0	6.0.0	R5-063574
RP-34	RP-060748	0030	-	Updates to TC 11.2 Network initiated re-authentication for IMS Rel-6	F	5.1.0	6.0.0	R5-063573
RP-34	RP-060748	0031	-	Updates to TC 12.1 MO Call Successful for IMS Rel-6	F	5.1.0	6.0.0	R5-063570
RP-34	RP-060748	0032	-	Updates to TC 8.1 Initial registration for IMS Rel-6	F	5.1.0	6.0.0	R5-063569
RP-35	RP-070088	0034	-	New TC 12.6	F	6.0.0	6.1.0	R5-070408
RP-35	RP-070088	0035	-	New TC 12.7	F	6.0.0	6.1.0	R5-070447
RP-35	RP-070088	0036	-	New TC 12.8	F	6.0.0	6.1.0	R5-070446
RP-35	RP-070088	0037	-	TC 8.5 Conformance requirement update	F	6.0.0	6.1.0	R5-070099
RP-35	RP-070088	0038	-	TC 8.6 Conformance requirement update	F	6.0.0	6.1.0	R5-070410
RP-35	RP-070088	0039	-	TC 8.7 Conformance requirement update	F	6.0.0	6.1.0	R5-070101
RP-35	RP-070088	0040	-	TC 12.2 Conformance requirement update	F	6.0.0	6.1.0	R5-070102
RP-35	RP-070088	0041	-	Corrections and updating default message according release 6	F	6.0.0	6.1.0	R5-070407
RP-35	RP-070088	0042	-	IMS security and early IMS security capability update	F	6.0.0	6.1.0	R5-070104

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-35	RP-070088	0043	-	Correct missing IMS security in TC 14.2	F	6.0.0	6.1.0	R5-070105
RP-35	RP-070088	0044	-	Rename TC 8.6 and 8.7 to include “IMS security” instead of “IMS support”	F	6.0.0	6.1.0	R5-070106
RP-35	RP-070088	0045	-	Updates to 34.229 TC 12.1	F	6.0.0	6.1.0	R5-070412
RP-35	RP-070088	0046	-	Corrections to P-CSCF Discovery (IPv4) test cases	F	6.0.0	6.1.0	R5-070413
RP-35	RP-070088	0047	-	New IMS CC test case for MO call initiation when MO UE supports and uses preconditions whereas MT UE does not support preconditions (TC 12.5).	F	6.0.0	6.1.0	R5-070414
RP-35	RP-070088	0048	-	Updates to TC 8.2 User Initiated Re-Registration for IMS Rel-6	F	6.0.0	6.1.0	R5-070415
RP-35	RP-070088	0049	-	Removal of IMS CC test cases 7.7 and 7.8	F	6.0.0	6.1.0	R5-070210
RP-35	RP-070088	0050	-	Update IMS default message content for 503 Service Unavailable response	F	6.0.0	6.1.0	R5-070416
RP-35	RP-070088	0051	-	Update Specific message Content for 503 response in IMS TCs 10.1 and 12.2.	F	6.0.0	6.1.0	R5-070417
RP-35	RP-070088	0052	-	Updates to TC 13.1 SigComp in the Initial registration for IMS Rel-6	F	6.0.0	6.1.0	R5-070418
RP-35	RP-070088	0053	-	Updates to TC 13.2 SigComp in the MO Call for IMS Rel-6	F	6.0.0	6.1.0	R5-070419
RP-35	RP-070089	0054	-	Updates to TC 13.3 SigComp in the MT Call for IMS Rel-6	F	6.0.0	6.1.0	R5-070420
RP-35	RP-070089	0055	-	Updates to TC 13.4 State creation before authentication for IMS Rel-6	F	6.0.0	6.1.0	R5-070421
RP-35	RP-070089	0056	-	Correction to test case 7.4	F	6.0.0	6.1.0	R5-070309
RP-35	RP-070089	0057	-	Rel-6 ISIM parameters	F	6.0.0	6.1.0	R5-070310
RP-35	RP-070089	0058	-	Updates to TC 12.4 Call initiation – Mobile termination for IMS Rel-6	F	6.0.0	6.1.0	R5-070424
RP-35	RP-070089	0059	-	Updates to TC 8.3 User initiated deregistration for IMS Rel-6	F	6.0.0	6.1.0	R5-070425
RP-36	RP-070362	0060	-	Usage of comp=sigcomp parameter in IMS TC 13.4	F	6.1.0	6.2.0	R5-071059
RP-36	RP-070362	0061	-	IMS TC 7.1: Additional option for coding the IPv4 address in PCO IE	F	6.1.0	6.2.0	R5-071437
RP-36	RP-070362	0062	-	Clarification on Require header in the UPDATE message for MT SigComp TC	F	6.1.0	6.2.0	R5-071489
RP-36	RP-070362	0063	-	Splitting MO Call TC 12.1 to Rel-5 and Rel-6 variants	F	6.1.0	6.2.0	R5-071496
RP-36	RP-070362	0064	-	Corrections and updates to TC 12.6	F	6.1.0	6.2.0	R5-071497
RP-36	RP-070362	0065	-	Corrections and updates to TC 12.7	F	6.1.0	6.2.0	R5-071498
RP-36	RP-070362	0066	-	Corrections and updates to TC 12.8	F	6.1.0	6.2.0	R5-071499
RP-36	RP-070362	0067	-	New TC MO Call (no resource reservation, preconditions used)	F	6.1.0	6.2.0	R5-071500
RP-36	RP-070362	0068	-	New TC MT Call (no resource reservation, preconditions used)	F	6.1.0	6.2.0	R5-071501
RP-36	RP-070362	0069	-	Clarification of test case purpose for TC 8.7 (wrong spec nr on the coversheet indicating 34.229-2, initially	F	6.1.0	6.2.0	R5-071488
RP-37	RP-070607	0070	-	Clarify parameter description in specific message contents	F	6.2.0	6.3.0	R5-072111
RP-37	RP-070607	0071	-	Update the SDP RFC reference	F	6.2.0	6.3.0	R5-072112
RP-37	RP-070607	0072	-	New TC User initiated re-registration for early IMS	F	6.2.0	6.3.0	R5-072113
RP-37	RP-070607	0073	-	Correction to IMS CC test case 12.4	F	6.2.0	6.3.0	R5-072119
RP-37	RP-070594	0074	-	Default message correction for 401 response	F	6.2.0	6.3.0	R5-072504
RP-37	RP-070594	0075	-	Correct check of ACK message in 12.9	F	6.2.0	6.3.0	R5-072508
RP-37	RP-070594	0076	-	Handling of optional PUBLISH messages	F	6.2.0	6.3.0	R5-072507
RP-37	RP-070607	0077	-	Correct the check of SDP answer to the SDP offer	F	6.2.0	6.3.0	R5-072511
RP-37	RP-070607	0078	-	Correct the re-invite message in 12.6	F	6.2.0	6.3.0	R5-072481
RP-37	RP-070594	0079	-	IMSCC Test 8.3 / Supported header in Register message for de-registration	F	6.2.0	6.3.0	R5-072505
RP-37	RP-070594	0080	-	Format of home domain name within the ISIM	F	6.2.0	6.3.0	R5-072506
RP-37	RP-070607	0081	-	New TC Mobile initiated de-registration for early IMS	F	6.2.0	6.3.0	R5-072495
RP-38	RP-070874	0087		IMS - Change of SUBSCRIBE Via header default value	F	6.3.0	6.4.0	R5-073468
RP-38	RP-070874	0086		Production of 34.229-1 pointer version in Rel-6 pointing to Rel-7 version	F	6.3.0	6.4.0	R5-073278
RP-38	RP-070882	0082		Updating references of 34.229-1 for MTSI and GRUU	F	6.3.0	7.0.0	R5-073036
RP-38	RP-070882	0083		Updating case 8.1 Initial Registration for 24.229 Rel-7	F	6.3.0	7.0.0	R5-073440
RP-38	RP-070882	0084		New IMS Rel-7 test case for MO MTSI voice call	F	6.3.0	7.0.0	R5-073298
RP-38	RP-070882	0085		New IMS Rel-7 test case for MO MTSI call hold	F	6.3.0	7.0.0	R5-073444
RP-39	RP-080113	0088		Centralizing rules for dialog identifiers to common messages	F	7.0.0	7.1.0	R5-080025

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-39	RP-080113	0089		Updating conformance requirements of registration test cases for Rel-7	F	7.0.0	7.1.0	R5-080026
RP-39	RP-080113	0090		Updating references of 34.229-1 to IETF RFCs related to MTSI	F	7.0.0	7.1.0	R5-080368
RP-39	RP-080113	0091		New Annex F for generic requirements of MTSI supplementary services	F	7.0.0	7.1.0	R5-080598
RP-39	RP-080113	0092		Update of common messages for MTSI communication service identifier	F	7.0.0	7.1.0	R5-080029
RP-39	RP-080113	0093		New MTSI test case 15.12 MT call hold	F	7.0.0	7.1.0	R5-080485
RP-39	RP-080113	0094		New MTSI test case 15.13 Incoming Communication Barring	F	7.0.0	7.1.0	R5-080031
RP-39	RP-080113	0095		New MTSI test case 15.23 MO Explicit Communication Transfer	F	7.0.0	7.1.0	R5-080486
RP-39	RP-080113	0096		IMS test case 8.3 / Supported Header and expire rule during de-registration	F	7.0.0	7.1.0	R5-080518
RP-39	RP-080113	0097		Align via header for early IMS	F	7.0.0	7.1.0	R5-080542
RP-39	RP-080113	0098		New MTSI test case MO MTSI Text call	F	7.0.0	7.1.0	R5-080547
RP-39	RP-080113	0099		New MTSI test case Speech AMR, indicate all codec modes	F	7.0.0	7.1.0	R5-080558
RP-39	RP-080113	0100		New MTSI test case Speech AMR-WB, indicate all codec modes	F	7.0.0	7.1.0	R5-080559
RP-39	RP-080113	0101		New MTSI test case MT Video, add speech remove speech	F	7.0.0	7.1.0	R5-080560
RP-39	RP-080113	0102		New MTSI test case MT Video, add speech remove video	F	7.0.0	7.1.0	R5-080561
RP-39	RP-080113	0103		Add generic secondary PDP context procedure	F	7.0.0	7.1.0	R5-080092
RP-39	RP-080113	0104		New MTSI test case for MO Consultative Explicit Communication Transfer	F	7.0.0	7.1.0	R5-080505
RP-39	RP-080113	0105		New MTSI test case for MT Consultative Explicit Communication Transfer	F	7.0.0	7.1.0	R5-080506
RP-40	RP-080375	0106		Updating references and ICSI statements related to MTSI	F	7.1.0	7.2.0	R5-081047
RP-40	RP-080375	0107		Fix to SDP handling in MTSI test case 16.3.	F	7.1.0	7.2.0	R5-081540
RP-40	RP-080375	0108		Branch value of Via header in MT messages	F	7.1.0	7.2.0	R5-081049
RP-40	RP-080375	0109		Introducing conditions for MO and MT versions of IMS common messages	F	7.1.0	7.2.0	R5-081050
RP-40	RP-080375	0110		New MTSI test case 15.6 Communication Deflection	F	7.1.0	7.2.0	R5-081539
RP-40	RP-080375	0111		New MTSI test case 15.17 Creating a conference	F	7.1.0	7.2.0	R5-081052
RP-40	RP-080375	0112		New MTSI test case 17.1 MO Speech add video remove video	F	7.1.0	7.2.0	R5-081541
RP-40	RP-080375	0113		New MTSI test case 15.5 Communication Forwarding unconditional	F	7.1.0	7.2.0	R5-081054
RP-40	RP-080375	0114		New MTSI test case 15.24 MT ECT - Blind Call Transfer	F	7.1.0	7.2.0	R5-081055
RP-40	RP-080375	0115		Update conformance requirement for TC 8.5	F	7.1.0	7.2.0	R5-081070
RP-40	RP-080375	0116		Update conformance requirement for TC 8.6	F	7.1.0	7.2.0	R5-081071
RP-40	RP-080375	0117		Update conformance requirement for TC 8.7	F	7.1.0	7.2.0	R5-081072
RP-40	RP-080375	0118		Update conformance requirement for TC 8.8	F	7.1.0	7.2.0	R5-081073
RP-40	RP-080375	0119		New MTSI test case MT MTSI Speech call	F	7.1.0	7.2.0	R5-081542
RP-40	RP-080375	0120		New MTSI test case MT MTSI Video call	F	7.1.0	7.2.0	R5-081543
RP-40	RP-080375	0121		New MTSI test case Speech AMR indicate selective codec modes	F	7.1.0	7.2.0	R5-081553
RP-40	RP-080375	0122		New MTSI test case Speech AMR-WB indicate selective codec modes	F	7.1.0	7.2.0	R5-081545
RP-40	RP-080375	0123		New MTSI test case MT Speech add video remove video	F	7.1.0	7.2.0	R5-081546
RP-40	RP-080375	0124		New MTSI test case MT Speech add video remove speech	F	7.1.0	7.2.0	R5-081547
RP-40	RP-080375	0125		Updating the content of the default INVITE message to Rel-7	F	7.1.0	7.2.0	R5-081537
RP-40	RP-080427	0126		Correction to 380 Alternative Service message	F	7.1.0	7.2.0	R5-081538
RP-41	RP-080563	0127		Add generic procedures for MTSI MT speech call, MT video call and MT text call	F	7.2.0	7.3.0	R5-083113
RP-41	RP-080563	0128		Update MTSI test case 12.13	F	7.2.0	7.3.0	R5-083114
RP-41	RP-080563	0129		Update MTSI test case 12.15	F	7.2.0	7.3.0	R5-083115
RP-41	RP-080563	0130		New MTSI test case 12.17 MT MTSI Text call	F	7.2.0	7.3.0	R5-083116
RP-41	RP-080563	0131		Update MTSI test case 16.1	F	7.2.0	7.3.0	R5-083126
RP-41	RP-080563	0132		Update MTSI test case 16.2	F	7.2.0	7.3.0	R5-083127
RP-41	RP-080563	0133		Update MTSI test case 16.3	F	7.2.0	7.3.0	R5-083128
RP-41	RP-080563	0134		Update MTSI test case 16.4	F	7.2.0	7.3.0	R5-083129
RP-41	RP-080563	0135		New MTSI test case 16.5 Video H.263 profile 0	F	7.2.0	7.3.0	R5-083130

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-41	RP-080563	0136		New MTSI test case 16.6 Video H.263 profile 3	F	7.2.0	7.3.0	R5-083131
RP-41	RP-080563	0137		New MTSI test case 16.7 Video H.264	F	7.2.0	7.3.0	R5-083132
RP-41	RP-080563	0138		New MTSI test case 16.8 Video MPEG-4	F	7.2.0	7.3.0	R5-083133
RP-41	RP-080563	0139		Update MTSI test case 12.16	F	7.2.0	7.3.0	R5-083392
RP-41	RP-080557	0140		Removal of IMS test case 13.4	F	7.2.0	7.3.0	R5-083489
RP-41	RP-080563	0141		New MTSI test case 17.12 MT Video, add text	F	7.2.0	7.3.0	R5-083554
RP-41	RP-080563	0142		New MTSI test case 17.18 MT Text, add video	F	7.2.0	7.3.0	R5-083557
RP-41	RP-080563	0143		Addition of new MTSI test case for Originating Identification Presentation	F	7.2.0	7.3.0	R5-083558
RP-41	RP-080563	0144		Addition of new MTSI test case for Origination Identification Restriction	F	7.2.0	7.3.0	R5-083559
RP-41	RP-080563	0145		Update MTSI test case 17.2	F	7.2.0	7.3.0	R5-083627
RP-41	RP-080563	0146		Update MTSI test case 17.4	F	7.2.0	7.3.0	R5-083628
RP-41	RP-080563	0147		Update MTSI test case 17.8	F	7.2.0	7.3.0	R5-083629
RP-41	RP-080563	0148		Update MTSI test case 17.10	F	7.2.0	7.3.0	R5-083630
RP-41	RP-080563	0149		New MTSI test case 17.14 MT Text, add speech remove speech	F	7.2.0	7.3.0	R5-083631
RP-41	RP-080563	0150		New MTSI test case 17.16 MT Text, add speech remove text	F	7.2.0	7.3.0	R5-083632
RP-41	RP-080563	0151		New MTSI test case 17.6 MT Speech, add text	F	7.2.0	7.3.0	R5-083119
RP-42	RP-080966	0152		Removing unnecessary exceptions from MTSI test case 12.4.	F	7.3.0	7.4.0	R5-085040
RP-42	RP-080966	0153		Updating generic requirements and XCAP test cases for XCAP authentication	F	7.3.0	7.4.0	R5-085041
RP-42	RP-080966	0154		New MTSI test case 15.14 Incoming Communication Barring for anonymous users	F	7.3.0	7.4.0	R5-085043
RP-42	RP-080966	0155		New MTSI test case 15.7 Communication Forwarding on non Reply: activation	F	7.3.0	7.4.0	R5-085044
RP-42	RP-080966	0156		New MTSI test case 15.21 Joining a conference after being invited to it	F	7.3.0	7.4.0	R5-085046
RP-42	RP-080966	0157		New MTSI test case 15.8 Communication Forwarding on non Reply: MO call initiation	F	7.3.0	7.4.0	R5-085047
RP-42	RP-080966	0158		Corrections to IMS CC test case 11.2 Network initiated re-authentication	F	7.3.0	7.4.0	R5-085050
RP-42	RP-080966	0159		Update 12.13 MT MTSI speech call	F	7.3.0	7.4.0	R5-085265
RP-42	RP-080966	0160		Update annex C.11 MTSI MT speech call	F	7.3.0	7.4.0	R5-085266
RP-42	RP-080966	0161		Add chapter headings for chapter 16 and 17	F	7.3.0	7.4.0	R5-085267
RP-42	RP-080966	0162		Correction to add the reference to the PICS statements in Annex A	F	7.3.0	7.4.0	R5-085341
RP-42	RP-080966	0163		Remove non MTSI related call setup test cases	F	7.3.0	7.4.0	R5-085350
RP-42	RP-080966	0164		Clarify GRUU applicability	F	7.3.0	7.4.0	R5-085351
RP-42	RP-080966	0165		Add generic procedures for MTSI MO speech call, call hold and conference call	F	7.3.0	7.4.0	R5-085405
RP-42	RP-080966	0166		New MTSI test case 16.10 MO MTSI Text session with MSRP	F	7.3.0	7.4.0	R5-085406
RP-42	RP-080966	0167		Update 16.1 Speech AMR, indicate all codec modes	F	7.3.0	7.4.0	R5-085426
RP-42	RP-080966	0168		Update 16.2 Speech AMR, indicate selective codec modes	F	7.3.0	7.4.0	R5-085427
RP-42	RP-080966	0169		Update 16.3 Speech AMR-WB, indicate all codec modes	F	7.3.0	7.4.0	R5-085428
RP-42	RP-080966	0170		Update 16.4 Speech AMR-WB, indicate selective codec mode	F	7.3.0	7.4.0	R5-085429
RP-42	RP-080966	0171		Update 17.2 MT Speech, add video remove video	F	7.3.0	7.4.0	R5-085432
RP-42	RP-080966	0172		Update of MTSI test cases for adding/removing media	F	7.3.0	7.4.0	R5-085443
RP-42	RP-080966	0173		New MTSI test case 15.18 Inviting user to conference by sending a REFER request to the user	F	7.3.0	7.4.0	R5-085445
RP-42	RP-080966	0174		Remove MTSI test cases for non mandatory use cases	F	7.3.0	7.4.0	R5-085446
RP-43	RP-090205	0175	-	Update of TS 34.229-1 from Rel-7 to Rel-8		7.4.0	8.0.0	R5-090763
RP-43	RP-090213	0202	-	IMS test case 8.9 / Supported Header and expire rule during de-registration		8.0.0	8.1.0	R5-090206
RP-43	RP-090213	0176	-	Addition of new MTSI test case for Terminating Identification Presentation		8.0.0	8.1.0	R5-090545
RP-43	RP-090213	0177	-	Addition of new MTSI test case for Terminating Identification Restriction		8.0.0	8.1.0	R5-090546
RP-43	RP-090213	0178	-	Updates to MTSI TCs 12.12 and 17.1 for MO speech and video		8.0.0	8.1.0	R5-090584
RP-43	RP-090213	0179	-	New MTSI test case 15.19 for inviting user to conference via conference focus		8.0.0	8.1.0	R5-090593
RP-43	RP-090213	0180	-	New MTSI test case 15.9 Communication Forwarding on Busy		8.0.0	8.1.0	R5-090594

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-43	RP-090213	0181	-	New MTSI test case 15.10 Communication Forwarding not logged in		8.0.0	8.1.0	R5-090595
RP-43	RP-090213	0182	-	New MTSI test case 15.15 Subscription to the MWI event package		8.0.0	8.1.0	R5-090596
RP-43	RP-090213	0183	-	New MTSI test case 17.5 MO Speech, add text		8.0.0	8.1.0	R5-090597
RP-43	RP-090213	0184	-	Harmonizing the requirements within MTSI XCAP test cases		8.0.0	8.1.0	R5-090598
RP-43	RP-090213	0185	-	Add annex MTSI MT speech call, SS resources available		8.0.0	8.1.0	R5-090599
RP-43	RP-090213	0186	-	New MTSI test case 16.11		8.0.0	8.1.0	R5-090600
RP-43	RP-090213	0187	-	New MTSI test case 16.12		8.0.0	8.1.0	R5-090601
RP-43	RP-090213	0188	-	Remove video only based codec selection test cases		8.0.0	8.1.0	R5-090603
RP-43	RP-090213	0189	-	Update MTSI test case 17.2		8.0.0	8.1.0	R5-090613
RP-43	RP-090213	0190	-	Update MTSI test case 17.6		8.0.0	8.1.0	R5-090614
RP-43	RP-090213	0191	-	Update MTSI test case 17.18		8.0.0	8.1.0	R5-090615
RP-43	RP-090213	0192	-	Add annex MTSI MO text call		8.0.0	8.1.0	R5-090617
RP-43	RP-090213	0193	-	Update MTSI test case 12.16		8.0.0	8.1.0	R5-090618
RP-43	RP-090213	0194	-	New MTSI test case 17.17		8.0.0	8.1.0	R5-090619
RP-43	RP-090213	0195	-	Update annex C.11 MTSI MT speech call		8.0.0	8.1.0	R5-090620
RP-43	RP-090214	0196	-	Update annex C.13 MTSI MT text call		8.0.0	8.1.0	R5-090621
RP-43	RP-090214	0197	-	Update MTSI test case 12.13		8.0.0	8.1.0	R5-090622
RP-43	RP-090214	0198	-	Update MTSI test case 12.17		8.0.0	8.1.0	R5-090623
RP-43	RP-090214	0199	-	New MTSI test case 16.13		8.0.0	8.1.0	R5-090660
RP-43	RP-090214	0200	-	Remove non MTSI related call setup test cases (2nd)		8.0.0	8.1.0	R5-090661
RP-43	RP-090214	0201	-	Remove MTSI test case 17.8		8.0.0	8.1.0	R5-090662
RP-44	RP-090433	0202	-	Update IMS test case 8.1, 8.2 and 8.6 with registration expire requirements		8.1.0	8.2.0	R5-092062
RP-44	RP-090433	0203	-	Update IMS test case 8.3 and 8.9 with registration expire requirements		8.1.0	8.2.0	R5-092063
RP-44	RP-090433	0204	-	Update IMS test case 8.5, 8.7 and 8.8 with registration expire requirements		8.1.0	8.2.0	R5-092064
RP-44	RP-090433	0205	-	Correction of registration expire requirements in annex A		8.1.0	8.2.0	R5-092065
RP-44	RP-090433	0206	-	Update of MTSI test case 15.15		8.1.0	8.2.0	R5-092217
RP-44	RP-090433	0207	-	Correction of MTSI icsi requirements		8.1.0	8.2.0	R5-092566
RP-45	RP-090794	0208	-	Update test cases 16.1, 16.2, 16.3 and 16.4 with multiple SDP check	F	8.2.0	8.3.0	R5-094352
RP-45	RP-090794	0209	-	Update annex C.13 and C.16 with multiple SDP check	F	8.2.0	8.3.0	R5-094353
RP-45	RP-090795	0210	-	Addition of P-Asserted-Identity header field to the 380 Alternative Service message	F	8.2.0	8.3.0	R5-094440
RP-46	RP-091118	0211		Update SDP speech offer for test case 12.13, annex C.11 and C.16	F	8.3.0	8.4.0	R5-095806
RP-46	RP-091118	0212	-	Update SDP speech offer for test cases 15.6	F	8.3.0	8.4.0	R5-095807
RP-46	RP-091118	0213	-	Update SDP speech offer for test cases 16.1, 16.2, 16.3 and 16.4	F	8.3.0	8.4.0	R5-095808
RP-46	RP-091118	0214	-	Update SDP speech offer for test cases 17.2 and 17.6	F	8.3.0	8.4.0	R5-095809
RP-46	RP-091118	0215	-	Correct gruu requirements in annex A	F	8.3.0	8.4.0	R5-095810
RP-46	RP-091116	0216	-	Update test case 14.2 with XML correction	F	8.3.0	8.4.0	R5-095812
RP-46	RP-091116	0217	-	Correct XML schema in 380 Alternative Service message	F	8.3.0	8.4.0	R5-095813
RP-46	RP-091118	0218	-	Update IMS test case 8.1, 8.5, 8.6 and 8.7 with registration expire corrections	F	8.3.0	8.4.0	R5-095816
RP-46	RP-091118	0219	-	Update IMS test case 8.1, 8.5, 8.6 and 8.7 with subscribe correction	F	8.3.0	8.4.0	R5-095817
RP-46	RP-091118	0220	-	Update test case 12.2	F	8.3.0	8.4.0	R5-096182
RP-46	RP-091118	0221	-	Update test cases 16.11, 16.12 and 16.13 with multiple SDP check	F	8.3.0	8.4.0	R5-096625
RP-46	RP-091118	0222	-	Update test cases 17.2, 17.6 and 17.18 with multiple SDP check	F	8.3.0	8.4.0	R5-096626
RP-47	RP-100155	0223	-	Add references for SMS over IP	F	8.4.0	8.5.0	R5-100505
RP-47	RP-100155	0224	-	Update message REGISTER for SMS	F	8.4.0	8.5.0	R5-100506
RP-47	RP-100155	0225	-	Update test case 8.1 for SMS	F	8.4.0	8.5.0	R5-100508
RP-47	RP-100155	0226	-	Add new test case 18.2 for SMS	F	8.4.0	8.5.0	R5-100509
RP-47	RP-100155	0227	-	Add default messages for SMS	F	8.4.0	8.5.0	R5-100785
RP-47	RP-100155	0228	1	Addition of new SMS over IMS test case 18.1	F	8.4.0	8.5.0	R5-101180
RP-47	-	-	-	Moved to v9.0.0 with no change	-	8.4.0	9.0.0	-
RP-48	RP-100511	0229	-	Update test cases 12.12 and 12.13 for AVP	F	9.0.0	9.1.0	R5-103485
RP-48	RP-100511	0230	-	Update generic procedure C.11 for AVP	F	9.0.0	9.1.0	R5-103490
RP-48	RP-100511	0231	-	Update test case 16.1 for AVP	F	9.0.0	9.1.0	R5-103492

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-48	RP-100511	0232	-	Update test case 16.2 for AVP	F	9.0.0	9.1.0	R5-103493
RP-48	RP-100511	0233	-	Update test case 16.3 for AVP	F	9.0.0	9.1.0	R5-103494
RP-48	RP-100511	0234	-	Update test case 16.4 for AVP	F	9.0.0	9.1.0	R5-103495
RP-48	RP-100511	0235	-	Aligning MTSI MO call towards GSMA VoLTE profile	F	9.0.0	9.1.0	R5-103853
RP-48	RP-100511	0238	-	Aligning MTSI Call Hold test cases towards GSMA VoLTE profile	F	9.0.0	9.1.0	R5-103854
RP-48	RP-100511	0236	-	Adding media and NoReplyTimer elements to MTSI TC 15.7	F	9.0.0	9.1.0	R5-103855
RP-48	RP-100511	0237	-	GCF Priority 4 - Correction to annex A for TC 18.1 SMS over IMS	F	9.0.0	9.1.0	R5-103857
RP-49	RP-100985	0249	-	Add new test case for user initiated de-registration using GIBA	F	9.1.0	9.2.0	R5-104433
RP-49	RP-100985	0255	-	Add new test case 15.X Communication Waiting and answering the call	F	9.1.0	9.2.0	R5-104740
RP-49	RP-100985	0245	-	Add generic procedure for EPS bearer context activation	F	9.1.0	9.2.0	R5-104311
RP-49	RP-100986	0252	-	Add new test case 15.X Three way session creation	F	9.1.0	9.2.0	R5-104522
RP-49	RP-100986	0244	-	Add generic procedure for PDP context activation	F	9.1.0	9.2.0	R5-104310
RP-49	RP-100986	0248	-	Add new test case for initial registration using IMS AKA and GIBA against a network with GIBA support only	F	9.1.0	9.2.0	R5-104431
RP-49	RP-100986	0247	-	Add new test case for initial registration using GIBA	F	9.1.0	9.2.0	R5-104430
RP-49	RP-100986	0242	-	Add new test case 15.x Communication Waiting and cancelling the call	F	9.1.0	9.2.0	R5-104292
RP-49	RP-100986	0253	-	Update generic procedures C.1, C.2 and C.2a	F	9.1.0	9.2.0	R5-104738
RP-49	RP-100986	0241	-	Add new test case 15.x Communication Forwarding not reachable	F	9.1.0	9.2.0	R5-104291
RP-49	RP-100986	0246	-	Remove clause 8 test cases for early IMS security	F	9.1.0	9.2.0	R5-104429
RP-49	RP-100986	0250	-	Update annex A for GIBA	F	9.1.0	9.2.0	R5-104434
RP-49	RP-100985	0251	-	Update test case 13.1	F	9.1.0	9.2.0	R5-104435
RP-49	RP-100986	0254	-	Add new test case for user initiated re-registration using GIBA	F	9.1.0	9.2.0	R5-104739
RP-49	RP-100986	0240	-	Correction to default Status Report for MO SMS	F	9.1.0	9.2.0	R5-104113
RP-49	RP-100985	0256	-	Changes to common messages for IMS emergency session setup	F	9.1.0	9.2.0	R5-105023
RP-49	RP-100838	0243	-	Update annex C.6	F	9.1.0	9.2.0	R5-104309
-	-	-	-	Editorial renumbering of test cases 15.27 - 15.30 in order to align with GCF list	-	9.1.0	9.2.0	-
RP-50	RP-101156	0260	-	Updates to conformance requirements related to IMS registration	F	9.2.0	9.3.0	R5-106152
RP-50	RP-101146	0258	-	Corrections to the conditions for using USIM or ISIM	F	9.2.0	9.3.0	R5-106150
RP-50	RP-101146	0259	-	Add new test case 15.14a Communication Barring while roaming	F	9.2.0	9.3.0	R5-106151
RP-50	RP-101146	0269	-	New Emergency test case 19.3.1 Non-UE detectable emergency call / IM CN sends a 1xx response / UE geographical location information available	F	9.2.0	9.3.0	R5-106590
RP-50	RP-101146	0268	-	Introducing TC 19.1.1 Basic IMS emergency call over EPS with emergency registration	F	9.2.0	9.3.0	R5-106586
RP-50	RP-101146	0262	-	Update of MTSI test cases 15.25 and 15.26	F	9.2.0	9.3.0	R5-106301
RP-50	RP-101146	0261	-	Update of MTSI test cases 15.1, 15.2, 15.3 and 15.4	F	9.2.0	9.3.0	R5-106300
RP-50	RP-101146	0264	-	Update to conformance requirement of PDP Context Activation test cases	F	9.2.0	9.3.0	R5-106470
RP-50	RP-101146	0263	-	Update conformance requirements for 8.10 and 8.11	F	9.2.0	9.3.0	R5-106452
RP-50	RP-101146	0267	-	Update test cases 9.1 and 9.2 to Rel-8	F	9.2.0	9.3.0	R5-106516
RP-50	RP-101146	0266	-	Remove test case 14.1 and 14.2	F	9.2.0	9.3.0	R5-106486
RP-50	RP-101156	0265	-	Update to conformance requirement of P-CSCF discovery test cases	F	9.2.0	9.3.0	R5-106472
RP-50	RP-101156	0257	-	Fixes to IMS common emergency messages	F	9.2.0	9.3.0	R5-106147
RP-50	RP-101146	0270	-	New IMS test case 12.2A MO Call - 504 Server Time-out	F	9.2.0	9.3.0	R5-106684
RP-51	RP-110165	0271	-	Updates to conformance requirements for XCAP and CDIV TCs	F	9.3.0	9.4.0	R5-110254
RP-51	RP-110165	0272	-	Updates to conformance requirements of IMS call related suppl. services	F	9.3.0	9.4.0	R5-110255
RP-51	RP-110165	0273	-	Updates to conformance requirements of IMS conference call TCs	F	9.3.0	9.4.0	R5-110256
RP-51	RP-110165	0274	-	Updates to conformance requirements of IMS MO calls	F	9.3.0	9.4.0	R5-110258
RP-51	RP-110165	0275	-	Updates to conformance requirements of IMS MO text session with MSRP	F	9.3.0	9.4.0	R5-110262
RP-51	RP-110174	0276	-	Corrections to the IMS emergency TC 19.1.1	F	9.3.0	9.4.0	R5-110265

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-51	RP-110174	0277	-	Introducing TC 19.5.6 User-initiated emergency reregistration / UE has emergency related ongoing dialog	F	9.3.0	9.4.0	R5-110266
RP-51	RP-110174	0278	-	Introducing TC 19.1.2 Emergency call with emergency registration / Success / Location information not available	F	9.3.0	9.4.0	R5-110267
RP-51	RP-110174	0279	-	Introducing TC 19.1.4 Emergency call with emergency registration / UE is not [normal] registered / Success	F	9.3.0	9.4.0	R5-110268
RP-51	RP-110165	0280	-	Update test case 10.1	F	9.3.0	9.4.0	R5-110366
RP-51	RP-110165	0281	-	Update test case 12.2	F	9.3.0	9.4.0	R5-110367
RP-51	RP-110165	0282	-	Update test case 12.13	F	9.3.0	9.4.0	R5-110368
RP-51	RP-110165	0283	-	Update test case 12.16	F	9.3.0	9.4.0	R5-110369
RP-51	RP-110165	0284	-	Update test case 12.17	F	9.3.0	9.4.0	R5-110370
RP-51	RP-110165	0285	-	Update test case 16.1	F	9.3.0	9.4.0	R5-110374
RP-51	RP-110165	0286	-	Update test case 16.2	F	9.3.0	9.4.0	R5-110375
RP-51	RP-110165	0287	-	Update test case 16.3	F	9.3.0	9.4.0	R5-110376
RP-51	RP-110165	0288	-	Update test case 16.4	F	9.3.0	9.4.0	R5-110377
RP-51	RP-110165	0289	-	Add editor's note to test case 16.11	F	9.3.0	9.4.0	R5-110493
RP-51	RP-110165	0290	-	Add editor's note to test case 16.12	F	9.3.0	9.4.0	R5-110494
RP-51	RP-110165	0291	-	Add editor's note to test case 16.13	F	9.3.0	9.4.0	R5-110495
RP-51	RP-110165	0292	-	Add editor's note to test case 17.2	F	9.3.0	9.4.0	R5-110496
RP-51	RP-110165	0293	-	Add editor's note to test case 17.6	F	9.3.0	9.4.0	R5-110497
RP-51	RP-110165	0294	-	Add editor's note to test case 17.17	F	9.3.0	9.4.0	R5-110498
RP-51	RP-110165	0295	-	Updating SMS related default messages and ISIM settings – 3 IMPU	F	9.3.0	9.4.0	R5-110673
RP-51	RP-110165	0296	-	Resubmission of new IMS test case 12.2A MO Call - 504 Server Time-out	F	9.3.0	9.4.0	R5-110689
RP-51	RP-110165	0297	-	Introducing new TC 7.9 P-CSCF discovery from ISIM	F	9.3.0	9.4.0	R5-110690
RP-51	RP-110165	0298	-	Correct service header fields in default MT INVITE	F	9.3.0	9.4.0	R5-110691
RP-51	RP-110165	0299	-	Support for multiple IMPU on ISIM	F	9.3.0	9.4.0	R5-110693
RP-51	RP-110165	0300	-	update test case 13.1	F	9.3.0	9.4.0	R5-110704
RP-51	RP-110165	0301	-	update test case 13.2	F	9.3.0	9.4.0	R5-110705
RP-51	RP-110165	0302	-	update test case 13.3	F	9.3.0	9.4.0	R5-110706
RP-51	RP-110174	0303	-	Introduction of new test case 19.1.3 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.3.0	9.4.0	R5-110804
RP-51	RP-110174	0304	-	Introduction of new test case 19.1.5 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.3.0	9.4.0	R5-110805
RP-51	RP-110174	0306	-	Introduction of new test case 19.4.3 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.3.0	9.4.0	R5-110807
RP-51	RP-110174	0307	-	Introduction of new test case 19.4.4 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.3.0	9.4.0	R5-110808
RP-51	RP-110174	0308	-	Update IMS emergency registration procedure	F	9.3.0	9.4.0	R5-110809
RP-51	RP-110174	0309	-	New emergency test case 19.3.2 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Non-emergency IMS registration	F	9.3.0	9.4.0	R5-110810
RP-52	RP-110660	0310	-	Removing references to MTSI from IMS emergency cal test cases	F	9.4.0	9.5.0	R5-112170
RP-52	RP-110660	0311	-	New TC 19.5.7 User-initiated emergency reregistration / The user initiates an emergency call	F	9.4.0	9.5.0	R5-112171
RP-52	RP-110660	0312	-	New TC 19.5.8 User-initiated emergency reregistration / Standalone transactions exist	F	9.4.0	9.5.0	R5-112172
RP-52	RP-110660	0313	-	New TC 19.5.9 In parallel emergency and non-emergency registrations	F	9.4.0	9.5.0	R5-112173
RP-52	RP-110660	0314	-	New TC 19.5.10 Deregistration upon emergency registration expiration	F	9.4.0	9.5.0	R5-112174
RP-52	RP-110651	0315	-	Removal of early IMS security in clause 6 test cases	F	9.4.0	9.5.0	R5-112401
RP-52	RP-110651	0316	-	Removal of early IMS security in clause 7 test cases	F	9.4.0	9.5.0	R5-112402
RP-52	RP-110660	0317	-	Corrections to test case 19.1.5	F	9.4.0	9.5.0	R5-112406
RP-52	RP-110651	0318	-	Add editors note to test case 17.18	F	9.4.0	9.5.0	R5-112441
RP-52	RP-110651	0319	-	Add generic procedure for E-UTRAN MO speech	F	9.4.0	9.5.0	R5-112488
RP-52	RP-110660	0320	-	Add generic procedure for E-UTRAN emergency speech	F	9.4.0	9.5.0	R5-112492
RP-52	RP-110660	0321	-	Add new test case 19.4.1	F	9.4.0	9.5.0	R5-112495
RP-52	RP-110651	0322	-	Replacing px_PublicUserIdentity with references to IMPUs on ISIM	F	9.4.0	9.5.0	R5-112644
RP-52	RP-110651	0323	-	New IMS TC 8.x Refresh for ISIM parameters	F	9.4.0	9.5.0	R5-112645
RP-52	RP-110660	0324	-	Introduction of new test case 19.5.1 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112649
RP-52	RP-110660	0325	-	Introduction of new test case 19.4.2 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112650

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-52	RP-110660	0326	-	Introduction of new test case 19.4.5 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112651
RP-52	RP-110660	0310	-	Removing references to MTSI from IMS emergency cal test cases	F	9.4.0	9.5.0	R5-112170
RP-52	RP-110660	0311	-	New TC 19.5.7 User-initiated emergency reregistration / The user initiates an emergency call	F	9.4.0	9.5.0	R5-112171
RP-52	RP-110660	0312	-	New TC 19.5.8 User-initiated emergency reregistration / Standalone transactions exist	F	9.4.0	9.5.0	R5-112172
RP-52	RP-110660	0313	-	New TC 19.5.9 In parallel emergency and non-emergency registrations	F	9.4.0	9.5.0	R5-112173
RP-52	RP-110660	0314	-	New TC 19.5.10 Deregistration upon emergency registration expiration	F	9.4.0	9.5.0	R5-112174
RP-52	RP-110651	0315	-	Removal of early IMS security in clause 6 test cases	F	9.4.0	9.5.0	R5-112401
RP-52	RP-110651	0316	-	Removal of early IMS security in clause 7 test cases	F	9.4.0	9.5.0	R5-112402
RP-52	RP-110660	0317	-	Corrections to test case 19.1.5	F	9.4.0	9.5.0	R5-112406
RP-52	RP-110651	0318	-	Add editors note to test case 17.18	F	9.4.0	9.5.0	R5-112441
RP-52	RP-110651	0319	-	Add generic procedure for E-UTRAN MO speech	F	9.4.0	9.5.0	R5-112488
RP-52	RP-110660	0320	-	Add generic procedure for E-UTRAN emergency speech	F	9.4.0	9.5.0	R5-112492
RP-52	RP-110660	0321	-	Add new test case 19.4.1	F	9.4.0	9.5.0	R5-112495
RP-52	RP-110651	0322	-	Replacing px_PublicUserIdentity with references to IMPUs on ISIM	F	9.4.0	9.5.0	R5-112644
RP-52	RP-110651	0323	-	New IMS TC 8.x Refresh for ISIM parameters	F	9.4.0	9.5.0	R5-112645
RP-52	RP-110660	0324	-	Introduction of new test case 19.5.1 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112649
RP-52	RP-110660	0325	-	Introduction of new test case 19.4.2 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112650
RP-52	RP-110660	0326	-	Introduction of new test case 19.4.5 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112651
RP-53	RP-111142	0327	-	Update generic procedure for MTSI MO speech	F	9.5.0	9.6.0	R5-113735
RP-53	RP-111145	0328	-	Update generic procedures for IMS emergency call	F	9.5.0	9.6.0	R5-113740
RP-53	RP-111145	0329	-	Update test case 19.4.1	F	9.5.0	9.6.0	R5-113741
RP-53	RP-111151	0330	-	Addition of new test case 12.18	F	9.5.0	9.6.0	R5-113742
RP-53	RP-111151	0331	-	Addition of new test case 12.20	F	9.5.0	9.6.0	R5-113745
RP-54	RP-111583	0332	-	IMS Route header correction	F	9.6.0	9.7.0	R5-115326
RP-54	RP-111583	0333	-	Update annex C.21	F	9.6.0	9.7.0	R5-115341
RP-54	RP-111583	0334	-	Update test case 8.14	F	9.6.0	9.7.0	R5-115342
RP-54	RP-111583	0335	-	Update test case 12.2	F	9.6.0	9.7.0	R5-115343
RP-54	RP-111583	0336	-	Update test case and numbering to 12.2a	F	9.6.0	9.7.0	R5-115344
RP-54	RP-111583	0337	-	Update test case 12.12	F	9.6.0	9.7.0	R5-115346
RP-54	RP-111583	0338	-	Update test case 12.13	F	9.6.0	9.7.0	R5-115349
RP-54	RP-111583	0339	-	Update test case 15.8	F	9.6.0	9.7.0	R5-115493
RP-54	RP-111583	0340	-	Update test case 15.12	F	9.6.0	9.7.0	R5-115500
RP-54	RP-111583	0341	-	Add editor's note to annex C.7	F	9.6.0	9.7.0	R5-115513
RP-54	RP-111583	0342	-	Update test case 15.23	F	9.6.0	9.7.0	R5-115524
RP-54	RP-111583	0343	-	Removal of an editor's note for ISIM REFRESH	F	9.6.0	9.7.0	R5-115665
RP-54	RP-111583	0344	-	Update test case 15.11	F	9.6.0	9.7.0	R5-115666
RP-54	RP-111583	0345	-	Update test case 15.21a	F	9.6.0	9.7.0	R5-115667
RP-54	RP-111583	0346	-	Update test case 15.25	F	9.6.0	9.7.0	R5-115668
RP-54	RP-111583	0347	-	Update test case 15.26	F	9.6.0	9.7.0	R5-115669
RP-54	RP-111591	0348	-	Updating E-UTRA procedures for IMS emergency test cases	F	9.6.0	9.7.0	R5-115671
RP-55	RP-120184	0351	-	Update default message INVITE for MO	F	9.7.0	9.8.0	R5-120387
RP-55	RP-120184	0352	-	Add generic procedure for SRVCC media removal	F	9.7.0	9.8.0	R5-120392
RP-55	RP-120184	0353	-	Update annex C.22	F	9.7.0	9.8.0	R5-120399
RP-55	RP-120192	0354	-	Update of IMS emergency call test cases 19.1.3 and 19.1.5	F	9.7.0	9.8.0	R5-120405
RP-55	RP-120192	0355	-	Update of IMS emergency call test case 19.5.1	F	9.7.0	9.8.0	R5-120407
RP-55	RP-120183	0356	-	GCF Priority X - Correction to the test procedure in the section of 7.3.4	F	9.7.0	9.8.0	R5-120678
RP-55	RP-120183	0357	-	GCF Priority X - Correction to the test procedure in the section of 7.4.4, 7.5.4 and 7.6.4	F	9.7.0	9.8.0	R5-120679
RP-55	RP-120183	0358	-	GCF Priority X - Correction to the test procedures of the section of 12.2 and 12.2a	F	9.7.0	9.8.0	R5-120680
RP-55	RP-120183	0359	-	GCF Priority X - Correction to the message content in the section of 13.2.4	F	9.7.0	9.8.0	R5-120681

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-55	RP-120183	0360	-	GCF Priority X - Correction to the testing sequence numberings in the sections of 15.21a and 15.23	F	9.7.0	9.8.0	R5-120682
RP-55	RP-120183	0361	-	GCF Priority X - Correction to the testing sequence numberings in the sections of 15.27	F	9.7.0	9.8.0	R5-120683
RP-55	RP-120183	0362	-	GCF Priority X - Correction to the testing content of 17.17.4	F	9.7.0	9.8.0	R5-120684
RP-55	RP-120171	0363	-	GCF Priority X - Correction to the reference index	F	9.7.0	9.8.0	R5-120685
RP-55	RP-120184	0364	-	Update default message 183 Session Progress	F	9.7.0	9.8.0	R5-120686
RP-55	RP-120192	0365	-	Update of IMS emergency call test cases 19.4.x	F	9.7.0	9.8.0	R5-120691
RP-55	RP-120195	0366	-	Addition of new test case 12.19	F	9.7.0	9.8.0	R5-120722
RP-56	RP-120649	0367	-	Update test case 12.12	F	9.8.0	9.9.0	R5-121423
RP-56	RP-120649	0368	-	Update test case 12.13	F	9.8.0	9.9.0	R5-121424
RP-56	RP-120655	0369	-	Removing TC 19.1.4 from 34.229-1	F	9.8.0	9.9.0	R5-121430
RP-56	RP-120649	0370	-	Correction of XCAP MIME definition	F	9.8.0	9.9.0	R5-121629
RP-56	RP-120649	0371	-	Addition of new test case - MO MTSI Video Call	F	9.8.0	9.9.0	R5-121631
RP-56	RP-120649	0372	-	Addition of new test case - MT MTSI Video Call	F	9.8.0	9.9.0	R5-121633
RP-56	RP-120649	0373	-	Updates to 17.1 - MO Speech, add video remove video	F	9.8.0	9.9.0	R5-121635
RP-56	RP-120649	0374	-	Updates to 17.2 - MT Speech, add video remove video	F	9.8.0	9.9.0	R5-121636
RP-56	RP-120649	0375	-	Add generic procedure MT Video call for EPS	F	9.8.0	9.9.0	R5-121657
RP-56	RP-120648	0376	-	MO Message content correction for SMS-over-IMS	F	9.8.0	9.9.0	R5-121675
RP-56	RP-120649	0377	-	Add generic procedure MO video call for EPS	F	9.8.0	9.9.0	R5-121803
RP-56	RP-120655	0378	-	Correction to IMS emergency test case 19.3.2	F	9.8.0	9.9.0	R5-121804
RP-56	RP-120655	0379	-	New test case 19.3.3 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Emergency IMS registration	F	9.8.0	9.9.0	R5-121805
RP-56	RP-120655	0380	-	New test case 19.3.4 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Emergency IMS registration exists	F	9.8.0	9.9.0	R5-121806
RP-56	RP-120657	0381	-	Update the default messages and generic test procedures	F	9.8.0	9.9.0	R5-121851
RP-56	RP-120657	0382	-	Update to test case 12.19	F	9.8.0	9.9.0	R5-121852
RP-57	RP-121102	0383	-	IMS MTSI message content correction	F	9.9.0	9.10.0	R5-123077
RP-57	RP-121103	0384	-	Update to test case 12.19	F	9.9.0	9.10.0	R5-123200
RP-57	RP-121103	0385	-	Update generic procedure C.21	F	9.9.0	9.10.0	R5-123505
RP-57	RP-121103	0386	-	Update generic procedure C.25	F	9.9.0	9.10.0	R5-123525
RP-57	RP-121103	0387	-	Update generic procedure C.26	F	9.9.0	9.10.0	R5-123681
RP-57	RP-121103	0388	-	Update the default messages for IMS video	F	9.9.0	9.10.0	R5-123682
RP-57	RP-121103	0389	-	Updates to 17.1 - MO Speech, add video remove video	F	9.9.0	9.10.0	R5-123683
RP-57	RP-121103	0390	-	Updates to 17.2 - MT Speech, add video remove video	F	9.9.0	9.10.0	R5-123684
RP-58	RP-121663	0391	-	Correction of default message contents in Annex A	F	9.10.0	9.11.0	R5-125288
RP-58	RP-121663	0392	-	Correction of 11.2	F	9.10.0	9.11.0	R5-125289
RP-58	RP-121664	0393	-	Correction to references	F	9.10.0	9.11.0	R5-125575
RP-58	RP-121664	0394	-	Updates to 12-21 - MO MTSI Video call	F	9.10.0	9.11.0	R5-125578

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-58	RP-121664	0395	-	Updates to 12-22 - MT MTSI Video call	F	9.10.0	9.11.0	R5-125579
RP-58	RP-121664	0396	-	Updates to 17.1 - MO Speech, add video remove video	F	9.10.0	9.11.0	R5-125580
RP-58	RP-121664	0397	-	Updates to 17.2 - MT Speech, add video remove video	F	9.10.0	9.11.0	R5-125581
RP-58	RP-121664	0398	-	Update test case 19.5.6	F	9.10.0	9.11.0	R5-125588
RP-58	RP-121664	0399	-	Update test case 19.5.1	F	9.10.0	9.11.0	R5-125589
RP-58	RP-121664	0400	-	Update test case 19.5.7	F	9.10.0	9.11.0	R5-125590
RP-58	RP-121664	0401	-	Update test case 19.5.8	F	9.10.0	9.11.0	R5-125591
RP-58	RP-121664	0402	-	Update test case 19.5.10	F	9.10.0	9.11.0	R5-125592
RP-58	RP-121664	0403	-	Update test case 19.3.1	F	9.10.0	9.11.0	R5-125595
RP-58	RP-121664	0404	-	Update test case 19.1.5	F	9.10.0	9.11.0	R5-125616
RP-58	RP-121664	0405	-	Removal of location accuracy requirement from Emergency Services test cases	F	9.10.0	9.11.0	R5-125771
RP-58	RP-121664	0406	-	Update generic procedure C.11	F	9.10.0	9.11.0	R5-125772
RP-58	RP-121663	0407	-	IMS MTSI TC 15.28 correction	F	9.10.0	9.11.0	R5-125773
RP-58	RP-121663	0408	-	IMS MTSI TC 15.8 correction	F	9.10.0	9.11.0	R5-125774
RP-58	RP-121664	0411	-	Location stimulus clarification for Emergency Services test cases	F	9.10.0	9.11.0	R5-126025
RP-58	RP-121663	0412	-	IMS extend IMS_CC test case 8.1 for LTE	F	9.10.0	9.11.0	R5-126033
RP-58	RP-121663	0413	-	IMS Default content of ACK	F	9.10.0	9.11.0	R5-126034
RP-58	RP-121685	0409	-	Update the default messages for aSRVCC	F	9.11.0	10.0.0	R5-126003
RP-58	RP-121685	0410	-	Addition of new generic test procedures for aSRVCC	F	9.11.0	10.0.0	R5-126004
RP-59	RP-130145	0414	-	Correction to reference for IMS video related capability defined in TS 34.229-2	F	10.0.0	10.1.0	R5-130083
RP-59	RP-130143	0416	-	Update test case 12.21	F	10.0.0	10.1.0	R5-130491
RP-59	RP-130143	0417	-	Update test case 12.22	F	10.0.0	10.1.0	R5-130495
RP-59	RP-130143	0418	-	Update annex C.11	F	10.0.0	10.1.0	R5-130497
RP-59	RP-130143	0419	-	Correction to default settings of EF IMPU at ISIM ADF	F	10.0.0	10.1.0	R5-130519
RP-59	RP-130143	0420	-	Corrections to IMS_CC test case 8.4	F	10.0.0	10.1.0	R5-130548
RP-59	RP-130145	0421	-	Updates to conformance requirements in 19.1.1.2, 19.1.3.2, 19.1.5.2	F	10.0.0	10.1.0	R5-130566
RP-59	RP-130145	0422	-	Corrections to 19.5.6, 19.5.7, 19.5.8, A.1.1	F	10.0.0	10.1.0	R5-130567
RP-59	RP-130145	0423	-	Update A.7.2 MESSAGE for delivery report	F	10.0.0	10.1.0	R5-130572
RP-59	RP-130143	0424	-	Correction of 15 series of SS tests	F	10.0.0	10.1.0	R5-130678
RP-59	RP-130143	0425	-	Update test case 17.1	F	10.0.0	10.1.0	R5-130679
RP-59	RP-130143	0426	-	Update test case 17.2	F	10.0.0	10.1.0	R5-130680
RP-59	RP-130145	0427	-	Corrections to A.2.7	F	10.0.0	10.1.0	R5-130682
RP-59	RP-130145	0428	-	Corrections to A.3.1	F	10.0.0	10.1.0	R5-130683
RP-59	RP-130145	0429	-	Update default message MESSAGE for MO SMS	F	10.0.0	10.1.0	R5-130684
RP-59	RP-130145	0430	-	Update A.7.6 Delivery report for MO SMS	F	10.0.0	10.1.0	R5-130685
RP-59	RP-130143	0431	-	Update Annex A, C	F	10.0.0	10.1.0	R5-130750

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-59	RP-130143	0432	-	Correction to SDP parameter in Generic Procedures in Annex C	F	10.0.0	10.1.0	R5-130751
RP-60	R5-131132	0433	-	Correction of TC 15.1	F	10.1.0	10.2.0	R5-131132
RP-60	R5-131134	0434	-	Update Annex A.1	F	10.1.0	10.2.0	R5-131134
RP-60	R5-131135	0435	-	Add new generic procedures in Annex C.29 for Supplementary Services test	F	10.1.0	10.2.0	R5-131135
RP-60	R5-131138	0436	-	TC 19.1.3a & 19.3.2a - split 1xRTT from UTRA, GERAN	F	10.1.0	10.2.0	R5-131138
RP-60	R5-131167	0437	-	Update to test function Update UE Location Information	F	10.1.0	10.2.0	R5-131167
RP-60	R5-131170	0438	-	Add missing references	F	10.1.0	10.2.0	R5-131170
RP-60	R5-131269	0439	-	Misc changes for TC 18.1	F	10.1.0	10.2.0	R5-131269
RP-60	R5-131292	0440	-	TCP as normative DL transport protocol in IMS Registration test	F	10.1.0	10.2.0	R5-131292
RP-60	R5-131875	0441	-	Update test case 8.4	F	10.1.0	10.2.0	R5-131875
RP-60	R5-131887	0442	-	Expiry value in 200 OK	F	10.1.0	10.2.0	R5-131887
RP-60	R5-131897	0443	-	to-tag in ACK	F	10.1.0	10.2.0	R5-131897
RP-60	R5-132037	0444	-	Addition of new generic procedure in C.30 for Mobile Initiated IMS Deregistration	F	10.1.0	10.2.0	R5-132037
RP-60	R5-132038	0445	-	Correction of TC 8.2	F	10.1.0	10.2.0	R5-132038
RP-60	R5-132063	0446	-	To-tag in 202 Accepted	F	10.1.0	10.2.0	R5-132063
RP-60	R5-132064	0447	-	Record-Route header in A.2.3 on 183 Session Progress for INVITE	F	10.1.0	10.2.0	R5-132064
RP-60	R5-132065	0448	-	Fix step numbering in 9.2.4	F	10.1.0	10.2.0	R5-132065
RP-60	R5-132068	0449	-	Correction of TC 15.8	F	10.1.0	10.2.0	R5-132068
RP-61	RP-131100	0450	-	Correction to reference to RFC 6442	F	10.2.0	10.3.0	R5-133151
RP-61	RP-131100	0451	-	Correction to PRACK default message contents	F	10.2.0	10.3.0	R5-133188
RP-61	RP-131100	0452	-	Correction of TC 15 series	F	10.2.0	10.3.0	R5-133197
RP-61	RP-131100	0453	-	Correction of Annex C.29	F	10.2.0	10.3.0	R5-133198
RP-61	RP-131100	0454	-	Add MMI command releasing call in TC 12.12	F	10.2.0	10.3.0	R5-133301
RP-61	RP-131100	0455	-	Referring to generic procedure C.30 in TC 8.3	F	10.2.0	10.3.0	R5-133302
RP-61	RP-131100	0456	-	Correction of A.2.7	F	10.2.0	10.3.0	R5-133303
RP-61	RP-131100	0457	-	Clarification of A.2.9	F	10.2.0	10.3.0	R5-133304
RP-61	RP-131100	0458	-	Correction of C.30	F	10.2.0	10.3.0	R5-133305
RP-61	RP-131100	0459	-	Correction of the magic cookie value in Via branch as per the RFC 3261 definition	F	10.2.0	10.3.0	R5-133355
RP-61	RP-131100	0460	-	Restricting usage of rport to UDP as transport protocol	F	10.2.0	10.3.0	R5-133358
RP-61	RP-131100	0461	-	Correction to IMS Deregistration procedure in case of using TCP	F	10.2.0	10.3.0	R5-133578
RP-61	RP-131100	0462	-	Corrections to allow both ISIM or USIM to be used in IMS CC test cases	F	10.2.0	10.3.0	R5-133628
RP-61	RP-131100	0463	-	Correction of Option tags to indicate support of '100rel' and/or 'precondition'	F	10.2.0	10.3.0	R5-133629
RP-61	RP-131100	0464	-	Updating conformance requirements for test case 18.1	F	10.2.0	10.3.0	R5-133630
RP-61	RP-131100	0465	-	Clarification on SDP messages and SIP signalling of C.21	F	10.2.0	10.3.0	R5-133684
RP-61	RP-131100	0466	-	Clarification on SDP messages of C.13	F	10.2.0	10.3.0	R5-133703
RP-61	RP-131100	0467	-	Corrections to SMS over IMS test cases	F	10.2.0	10.3.0	R5-133705

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-62	RP-131861	0468	-	Correction to MESSAGE default contents for SMS over IMS	F	10.3.0	10.4.0	R5-134094
RP-62	RP-131861	0469	-	Correction to default contents of 100 Trying response	F	10.3.0	10.4.0	R5-134095
RP-62	RP-131861	0470	-	Editorial corrections and clarifications to test case 15.11	F	10.3.0	10.4.0	R5-134114
RP-62	RP-131861	0471	-	Editorial corrections and clarifications to test case 15.8	F	10.3.0	10.4.0	R5-134115
RP-62	RP-131861	0472	-	Corrections for A.2.8 (BYE)	F	10.3.0	10.4.0	R5-134116
RP-62	RP-131861	0473	-	Correction of expected sequence of C.26	F	10.3.0	10.4.0	R5-134118
RP-62	RP-131861	0474	-	Clarification on SDP messages of C.11	F	10.3.0	10.4.0	R5-134119
RP-62	RP-131875	0475	-	Editorial corrections for SMS default message content	F	10.3.0	10.4.0	R5-134120
RP-62	RP-131875	0476	-	Update C.11 for IR.92 version 7	F	10.3.0	10.4.0	R5-134270
RP-62	RP-131875	0477	-	Clarify check of encrypt-algorithm in annex A.	F	10.3.0	10.4.0	R5-134287
RP-62	RP-131863	0478	-	Remove not needed test cases	F	10.3.0	10.4.0	R5-134297
RP-62	RP-131863	0479	-	Correction of Emergency Service over IMS test case 19.1.3	F	10.3.0	10.4.0	R5-134385
RP-62	RP-131863	0480	-	Correction of Emergency Service over IMS test case 19.5.7	F	10.3.0	10.4.0	R5-134386
RP-62	RP-131861	0481	-	Correction of Emergency Service over IMS test case 19.5.8	F	10.3.0	10.4.0	R5-134387
RP-62	RP-131875	0482	-	Corrections and clarifications to C.29.1	F	10.3.0	10.4.0	R5-134455
RP-62	RP-131875	0483	-	Update annex C for SDP	F	10.3.0	10.4.0	R5-134617
RP-62	RP-131875	0484	-	Update annex A for SDP	F	10.3.0	10.4.0	R5-134627
RP-62	RP-131875	0485	-	Clarify SDP in annex C.21	F	10.3.0	10.4.0	R5-134630
RP-62	RP-131875	0486	-	Update test case 17.2	F	10.3.0	10.4.0	R5-134646
RP-62	RP-131875	0487	-	Update annex C.11 according AP#60.08	F	10.3.0	10.4.0	R5-134648
RP-62	RP-131861	0488	-	Correction to default messages	F	10.3.0	10.4.0	R5-134659
RP-62	RP-131861	0489	-	Enhancement of C.8 to support Call Resume	F	10.3.0	10.4.0	R5-134793
RP-62	RP-131861	0490	-	Editorial correction for C.22	F	10.3.0	10.4.0	R5-134795
RP-62	RP-131861	0491	-	Correction of expected sequence of 16.1 and 16.3	F	10.3.0	10.4.0	R5-134796
RP-62	RP-131863	0492	-	Correction of expected sequence of C.13	F	10.3.0	10.4.0	R5-134797
RP-62	RP-131863	0493	-	Alignment of IMS message definitions with RFC6442	F	10.3.0	10.4.0	R5-134798
RP-62	RP-131861	0494	-	Correction to Annex A.2.1 and A.2.3 IMS message for Emergency Call NoRegistration	F	10.3.0	10.4.0	R5-134955
RP-62	RP-131861	0495	-	Correction to contents of ACK in test case 12.2	F	10.3.0	10.4.0	R5-134958
RP-62	RP-131891	0496	-	Correction of rtpmap attributes for media in SDP answer	F	10.3.0	10.4.0	R5-134961
RP-62	RP-131861	0498	-	Record-Route header	F	10.3.0	10.4.0	R5-135004
RP-62	RP-131875	0499	-	Update C.21 for IR.92 version 7	F	10.3.0	10.4.0	R5-135020
RP-62	-	-	-	Moved to v11.0.0 with no change	-	10.4.0	11.0.0	-
RP-62	RP-131891	0497	-	Correction of note text for bSRVCC	F	11.0.0	12.0.0	R5-134962
RP-63	RP-140306	0500	-	Fixes to A.2.8 BYE	F	12.0.0	12.1.0	R5-140118
RP-63	RP-140306	0503	-	Fixes to C.11	F	12.0.0	12.1.0	R5-140135
RP-63	RP-140306	0504	-	P-Access-Network-Info header (PANI)	F	12.0.0	12.1.0	R5-140309

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-63	RP-140306	0505	-	Fixing prose related to TC 15.11	F	12.0.0	12.1.0	R5-140796
RP-63	RP-140306	0506	-	Minor corrections to TC 12.2	F	12.0.0	12.1.0	R5-140798
RP-63	RP-140306	0507	-	Unsuccessful SRVCC handover	F	12.0.0	12.1.0	R5-140799
RP-63	RP-140306	0508	-	Clarification for default message content for INVITE	F	12.0.0	12.1.0	R5-140901
RP-63	RP-140306	0510	-	from tag and to tag	F	12.0.0	12.1.0	R5-140903
RP-63	RP-140306	0511	-	Remove test case 16.1	F	12.0.0	12.1.0	R5-140904
RP-63	RP-140306	0512	-	Remove annex C.16	F	12.0.0	12.1.0	R5-140905
RP-63	RP-140306	0513	-	Clarify generic procedure C.21 for IR.92 7.0	F	12.0.0	12.1.0	R5-140906
RP-63	RP-140306	0514	-	Correct editorial errors in generic procedure C.21	F	12.0.0	12.1.0	R5-140907
RP-63	RP-140306	0515	-	Correction of GCF WI-103 MTSI Testcase 15.27	F	12.0.0	12.1.0	R5-140908
RP-63	RP-140306	0516	-	Correction to GCF WI-103 MTSI testcase 15.28	F	12.0.0	12.1.0	R5-140909
RP-63	RP-140334	0517	-	Addition of new TC for SSAC in Connected mode to voice call	F	12.0.0	12.1.0	R5-140910
RP-63	RP-140334	0518	-	Addition of new TC for SSAC in Connected mode changing to voice call	F	12.0.0	12.1.0	R5-140911
RP-63	RP-140334	0519	-	Addition of new TC of SSAC in Connected mode to video call	F	12.0.0	12.1.0	R5-140912
RP-63	RP-140334	0520	-	Addition of new TC of SSAC in Connected mode changing to video call	F	12.0.0	12.1.0	R5-140913
RP-63	RP-140334	0521	-	Addition of new TC of SSAC in Connected mode to emergency call	F	12.0.0	12.1.0	R5-140914
RP-63	RP-140306	0522	-	Fixing prose related to TC 15.12	F	12.0.0	12.1.0	R5-140915
RP-63	RP-140306	0523	-	Update test case 16.2 for IR.92	F	12.0.0	12.1.0	R5-140916
RP-63	RP-140306	0524	-	Update test case 16.4 for IR.92	F	12.0.0	12.1.0	R5-140917
RP-63	RP-140306	0525	-	Update test case 12.13 with SDP conformance requirement	F	12.0.0	12.1.0	R5-140919
RP-63	RP-140308	0526	-	Update of test case 19.3.3	F	12.0.0	12.1.0	R5-140920
RP-63	RP-140306	0527	-	Update generic procedure C.11 with SDP requirement	F	12.0.0	12.1.0	R5-140975
RP-63	RP-140306	0528	-	max-red	F	12.0.0	12.1.0	R5-141114
RP-63	RP-140306	0529	-	Corrections to default message content for ACK	F	12.0.0	12.1.0	R5-141115
RP-63	RP-140306	0509	-	Correction and addition of Generic Procedures in 34.229-1	F	12.0.0	12.1.0	R5-141128
RP-64	RP-140812	0530	-	Clarification for EFpsismsc on ISIM	F	12.1.0	12.2.0	R5-142157
RP-64	RP-140812	0531	-	PANI header in 200 OK	F	12.1.0	12.2.0	R5-142223
RP-64	RP-140812	0532	-	Corrections regarding URL encoding	F	12.1.0	12.2.0	R5-142247
RP-64	RP-140812	0533	-	Correction to test case 16.4	F	12.1.0	12.2.0	R5-142266
RP-64	RP-140817	0534	-	Correction of Invite Message for aSRVCC Testcases	F	12.1.0	12.2.0	R5-142287
RP-64	RP-140812	0535	-	Fixes to A.2.7 ACK	F	12.1.0	12.2.0	R5-142319
RP-64	RP-140812	0536	-	Record-Route header in MT re-INVITE requests	F	12.1.0	12.2.0	R5-142320
RP-64	RP-140812	0537	-	Clarification to test case 15.14a	F	12.1.0	12.2.0	R5-142486
RP-64	RP-140812	0538	-	Correct to delete semicolon (":") in the ecn media line format	F	12.1.0	12.2.0	R5-142519
RP-64	RP-140812	0539	-	Editorial correction to the reference document information on TC15.24.5	F	12.1.0	12.2.0	R5-142521
RP-64	RP-140817	0540	-	Add a reference to Release 10 UE in the "Reference" part	F	12.1.0	12.2.0	R5-142522

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-64	RP-140812	0541	-	Correct to the test step contents of the test cases 7.2 & 7.3	F	12.1.0	12.2.0	R5-142523
RP-64	RP-140812	0542	-	Correction to the typos in test cases from 7.2 to 7.6	F	12.1.0	12.2.0	R5-142524
RP-64	RP-140812	0543	-	Editorial update of TC 12.12	F	12.1.0	12.2.0	R5-142642
RP-64	RP-140815	0544	-	Corrections to clause 19 and Annex A.2.1	F	12.1.0	12.2.0	R5-142718
RP-64	RP-140812	0545	-	Editorial update of annex C	F	12.1.0	12.2.0	R5-142741
RP-64	RP-140812	0546	-	Test case 9.2: Clarification on meaning of “new Security-Client header”	F	12.1.0	12.2.0	R5-142929
RP-64	RP-140812	0547	-	Corrections to C.28	F	12.1.0	12.2.0	R5-142936
RP-64	RP-140812	0548	-	Restrict reason-text for unsuccessful SRVCC handover	F	12.1.0	12.2.0	R5-142948
RP-64	RP-140812	0549	-	No P-Preferred-Identity and Accept-Contact in re-INVITE requests	F	12.1.0	12.2.0	R5-142949
RP-64	RP-140815	0550	-	Correction of GCF WI-154 IMS Emergency Call Testcase 19.5.7	F	12.1.0	12.2.0	R5-142950
RP-64	RP-140812	0551	-	Corrections for Annex C.21	F	12.1.0	12.2.0	R5-142951
RP-64	RP-140812	0552	-	Correction to Annex procedure C.32 and C.33	F	12.1.0	12.2.0	R5-142952
RP-64	RP-140839	0553	-	Correction of SSAC in Connected mode TCs about RAB establishment	F	12.1.0	12.2.0	R5-142953
RP-64	RP-140815	0554	-	Addition of new TC for the UE behaviour receiving SIP_380	F	12.1.0	12.2.0	R5-142954
RP-64	RP-140812	0555	-	TC 15.27 disambiguation	F	12.1.0	12.2.0	R5-142955
RP-64	RP-140812	0556	-	Apply C.30 to TC 8.13	F	12.1.0	12.2.0	R5-142956
RP-64	RP-140812	0557	-	Remove annex C.7	F	12.1.0	12.2.0	R5-142957
RP-64	RP-140812	0558	-	Misc fixes to TC 12.2a	F	12.1.0	12.2.0	R5-142958
RP-64	RP-140812	0559	-	Fulfil AP#62.02 on TC 15.12 and C.9	F	12.1.0	12.2.0	R5-142993
RP-64	RP-140812	0560	-	Changes to 16.2, 16.3, and 16.4	F	12.1.0	12.2.0	R5-142994
RP-64	RP-140812	0561	-	Corrections to contents of SIP re-INVITE message	F	12.1.0	12.2.0	R5-142995
RP-64	RP-140812	0562	-	Fixes to o-lines in SDP bodies	F	12.1.0	12.2.0	R5-143201
RP-65	RP-141571	0563	-	Update the default security-client header field	F	12.2.0	12.3.0	R5-144131
RP-65	RP-141596	0564	-	Correction to SSAC test cases 12.18a, 12.19a, 12.20a	F	12.2.0	12.3.0	R5-144279
RP-65	RP-141571	0565	-	Corrections of test case 15.21	F	12.2.0	12.3.0	R5-144335
RP-65	RP-141571	0566	-	Corrections of SDP s= and o= lines in DL	F	12.2.0	12.3.0	R5-144402
RP-65	RP-141573	0567	-	Addition of new test case for SIP 423 against re-registration	F	12.2.0	12.3.0	R5-144547
RP-65	RP-141571	0568	-	New test case 15.19a Inviting user to conference by sending a REFER request to the conference focus / Video	F	12.2.0	12.3.0	R5-144556
RP-65	RP-141571	0569	-	New generic procedure C.37 for Generic test procedure for Inviting user to Video conference by sending a REFER request to the conference focus	F	12.2.0	12.3.0	R5-144561
RP-65	RP-141571	0570	-	New generic procedure C.38 for Generic test procedure for MTSI Video conference creation	F	12.2.0	12.3.0	R5-144564
RP-65	RP-141573	0571	-	Correction to Emergency Service over IMS test case 19.5.7	F	12.2.0	12.3.0	R5-144591
RP-65	RP-141571	0572	-	Correct video profile-level-id	F	12.2.0	12.3.0	R5-144595
RP-65	RP-141571	0573	-	Refining Record-Route header in MT re-INVITE requests	F	12.2.0	12.3.0	R5-144601
RP-65	RP-141571	0574	-	Correction to C.24 for SRVCC media removal	F	12.2.0	12.3.0	R5-144686
RP-65	RP-141571	0575	-	Addition of Generic test procedures C.34 and C.35 for removal of early dialog for originating call and incoming call for aSRVCC	F	12.2.0	12.3.0	R5-144687

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-65	RP-141596	0576	-	Editorial correction of title for Rel-12 SSAC	F	12.2.0	12.3.0	R5-144688
RP-65	RP-141571	0577	-	Add XUI requirements	F	12.2.0	12.3.0	R5-144689
RP-65	RP-141571	0578	-	New test case 15.11a MO Video Call Hold without announcement	F	12.2.0	12.3.0	R5-144690
RP-65	RP-141571	0579	-	New test case 15.12a MT Video Call Hold without announcement	F	12.2.0	12.3.0	R5-144691
RP-65	RP-141571	0580	-	New test case 15.21b Joining a conference after being invited to it / Video	F	12.2.0	12.3.0	R5-144693
RP-65	RP-141571	0581	-	New test case 15.21c Three way session creation / Video	F	12.2.0	12.3.0	R5-144695
RP-65	RP-141571	0582	-	Bandwidth values in SDP offered by SS	F	12.2.0	12.3.0	R5-144700
RP-65	RP-141571	0583	-	Correction to Initial registration using GIBA test case 8.10	F	12.2.0	12.3.0	R5-144701
RP-65	RP-141571	0584	-	Removal of px_pcscf	F	12.2.0	12.3.0	R5-144709
RP-65	RP-141573	0585	-	Correction to test case 19.1.3b	F	12.2.0	12.3.0	R5-144748
RP-65	RP-141571	0586	-	Reverting the coding changes to P-Asserted-Service and P-Preferred-Service	F	12.2.0	12.3.0	R5-144752
RP-65	RP-141571	0587	-	On SDP in re-INVITE requests in IMS test cases 15.11 and 15.12	F	12.2.0	12.3.0	R5-144753
RP-65	RP-141571	0588	-	Synch failure in IMS TC 9.2: Revisited	F	12.2.0	12.3.0	R5-144754
RP-65	RP-141571	0589	-	Clarification for SDP session-version field in Annex C.27	F	12.2.0	12.3.0	R5-144755
RP-66	RP-141761	0566	1	Re-implementing the RAN5 agreed CR R5-144402	F	12.3.0	12.4.0	-
RP-66	RP-142054	0590	-	Update of pre-alerting Feature-Caps header field in 183 session progress for bSRVCC test cases	F	12.3.0	12.4.0	R5-145071
RP-66	RP-142054	0591	-	Corrections for test case 17.2	F	12.3.0	12.4.0	R5-145194
RP-66	RP-142054	0592	-	unicast-address on o-line in SDP	F	12.3.0	12.4.0	R5-145261
RP-66	RP-142056	0593	-	Correction to IMS test case 8.16	F	12.3.0	12.4.0	R5-145369
RP-66	RP-142056	0594	-	Correction to IMS Emergency Call test case 19.5.7	F	12.3.0	12.4.0	R5-145546
RP-66	RP-142054	0595	-	IMS over UTRAN / Clarification of NSAPI value used for TCs 6.3 and 7.1	F	12.3.0	12.4.0	R5-145719
RP-66	RP-142054	0596	-	Correction to WI-103 IMS XCAP Testcase 15.5,15.7,15.9	F	12.3.0	12.4.0	R5-145720
RP-66	RP-142054	0597	-	Correction to GCF WI-103 IMS XCAP Testcases 15.14, 15.14a	F	12.3.0	12.4.0	R5-145721
RP-66	RP-142054	0598	-	Correction to WI-103 IMS XCAP Testcase 15.10a	F	12.3.0	12.4.0	R5-145722
RP-66	RP-142054	0599	-	Corrections for test case 17.1	F	12.3.0	12.4.0	R5-145723
RP-66	RP-142054	0600	-	Correction for pAccessNetworkInfo in SIP responses	F	12.3.0	12.4.0	R5-145724
RP-66	RP-142054	0601	-	Correction for SDP message contents for MO call setup	F	12.3.0	12.4.0	R5-145725
RP-66	RP-142054	0602	-	SDP in re-INVITE for Call Hold: revisited	F	12.3.0	12.4.0	R5-145726
RP-66	RP-142054	0603	-	Correction to IMS default message: port in Via header	F	12.3.0	12.4.0	R5-145727
RP-66	RP-142054	0604	-	Alignment of IMS TCs 16.2, 16.3, and 16.4	F	12.3.0	12.4.0	R5-145728
RP-66	RP-142054	0605	-	Target URI for Call Forwarding via XCAP	F	12.3.0	12.4.0	R5-145729
RP-66	RP-142054	0606	-	Issues on bandwidth modifiers RR and RR in SDP	F	12.3.0	12.4.0	R5-145730
RP-66	RP-142056	0607	-	Correction to WI-154 IMS Emergency Call Testcase 19.5.7	F	12.3.0	12.4.0	R5-145732
RP-66	RP-142056	0608	-	Introduction of test case 19.3.2c	F	12.3.0	12.4.0	R5-145733
RP-66	RP-142056	0609	-	Correction to IMS Emergency Call test case 19.3.3	F	12.3.0	12.4.0	R5-145734
RP-66	RP-142056	0610	-	Correction to WI-154 IMS Emergency Call testcase 19.3.4	F	12.3.0	12.4.0	R5-145735

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-66	RP-142073	0611	-	Addition of default messages contents exchange of ATGW information for rSRVCC	F	12.3.0	12.4.0	R5-145745
RP-66	RP-142073	0612	-	Updates of default message contents for IMS MO call setup for rSRVCC	F	12.3.0	12.4.0	R5-145746
RP-66	RP-142073	0613	-	New generic procedure for setting up MTSI MO speech call for rSRVCC	F	12.3.0	12.4.0	R5-145747
RP-66	RP-142073	0614	-	New generic procedure Generic test procedure for MTSI MT speech call for rSRVCC û user reject	F	12.3.0	12.4.0	R5-145748
RP-66	RP-142073	0615	-	New generic procedure Generic test procedure for MTSI MT speech call for rSRVCC in alerting state	F	12.3.0	12.4.0	R5-145749
RP-66	RP-142073	0616	-	New generic procedure for UE receiving the ATGW information for CS to PS SRVCC	F	12.3.0	12.4.0	R5-145750
RP-66	RP-142056	0617	-	Correction GCF WI-154 IMS Emergency Call Testcase 19.1.3	F	12.3.0	12.4.0	R5-145752
RP-66	RP-142054	0618	-	Updates to generic test procedure C.29.1	F	12.3.0	12.4.0	R5-145789
RP-66	RP-142073	0619	-	Updates of default message contents for IMS registration for rSRVCC	F	12.3.0	12.4.0	R5-145796
RP-67	RP-150325	0620	-	Correction to IMS test case 8.16	F	12.4.0	12.5.0	R5-150128
RP-67	RP-150325	0621	-	Correction to Test case 19.5.8	F	12.4.0	12.5.0	R5-150247
RP-67	RP-150322	0622	-	Correction to Test case 15.10a	F	12.4.0	12.5.0	R5-150248
RP-67	RP-150325	0623	-	Correction to Test case 19.5.7	F	12.4.0	12.5.0	R5-150250
RP-67	RP-150325	0624	-	Add reference document of RFC4488	F	12.4.0	12.5.0	R5-150251
RP-67	RP-150322	0625	-	Correction to GCF WI-154 IMS Emergency call Testcase 19.5.7	F	12.4.0	12.5.0	R5-150267
RP-67	RP-150322	0626	-	Correction to GCF WI-154 IMS Emergency call Testcases	F	12.4.0	12.5.0	R5-150268
RP-67	RP-150325	0627	-	Correction to IMS Emergency Call test case 19.1.5	F	12.4.0	12.5.0	R5-150338
RP-67	RP-150325	0628	-	Correction to IMS Emergency Call test case 19.5.7	F	12.4.0	12.5.0	R5-150345
RP-67	RP-150322	0629	-	Three way session creation	F	12.4.0	12.5.0	R5-150384
RP-67	RP-150322	0630	-	Updating RFC 4244 to RFC 7044	F	12.4.0	12.5.0	R5-150385
RP-67	RP-150322	0631	-	s-lines in SDP	F	12.4.0	12.5.0	R5-150386
RP-67	RP-150340	0632	-	Updates to A.1 default REGISTER messages	F	12.4.0	12.5.0	R5-150584
RP-67	RP-150340	0633	-	Updates to A.8 default messages for CS to PS SRVCC	F	12.4.0	12.5.0	R5-150585
RP-67	RP-150340	0634	-	Updates to annex C.39	F	12.4.0	12.5.0	R5-150586
RP-67	RP-150322	0635	-	Contact header in UPDATE requests	F	12.4.0	12.5.0	R5-150692
RP-67	RP-150322	0636	-	Correction for generic test procedure for IMS MO call	F	12.4.0	12.5.0	R5-150694
RP-67	RP-150340	0637	-	Correction to the procedure of C.40	F	12.4.0	12.5.0	R5-150696
RP-67	RP-150325	0638	-	Correction to the inconsistency in 19.1.3a	F	12.4.0	12.5.0	R5-150698
RP-67	RP-150325	0639	-	Correction to the missing part on TC19.3.2	F	12.4.0	12.5.0	R5-150699
RP-67	RP-150325	0640	-	Correction to IMS Emergency Call test case 19.1.3	F	12.4.0	12.5.0	R5-150700
RP-67	RP-150322	0641	-	Updating draft-montemurro-gsma-imei-urn to RFC	F	12.4.0	12.5.0	R5-150701
RP-67	RP-150322	0642	-	Addressing Action Point AP#65.02 on o-lines in SDP	F	12.4.0	12.5.0	R5-150702
RP-67	RP-150322	0643	-	Correction to GCF WI-198 IMS Video call Testcase 12.22	F	12.4.0	12.5.0	R5-150703
RP-67	RP-150325	0644	-	Correction to test case 19.3.2b	F	12.4.0	12.5.0	R5-150704
RP-67	RP-150322	0645	-	Corrections to IMS test case 15.15	F	12.4.0	12.5.0	R5-150705
RP-67	RP-150322	0646	-	ACK request in C.31	F	12.4.0	12.5.0	R5-150706

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-67	RP-150322	0647	-	183 Session Progress in TC 15.8	F	12.4.0	12.5.0	R5-150707
RP-67	RP-150322	0648	-	Add test case for GBA	F	12.4.0	12.5.0	R5-150708
RP-67	RP-150322	0649	-	Directionality attribute in MO and MT calls	F	12.4.0	12.5.0	R5-150709
RP-67	RP-150322	0650	-	Update annex C.29.2	F	12.4.0	12.5.0	R5-150711
RP-67	RP-150340	0651	-	Updates to annex C.40	F	12.4.0	12.5.0	R5-150713
RP-67	RP-150340	0652	-	Updates to annex C.42	F	12.4.0	12.5.0	R5-150714
RP-67	RP-150322	0653	-	Correction to C.25 - Generic test procedure for setting up MTSI MO video call for EPS	F	12.4.0	12.5.0	R5-150734
RP-67	RP-150322	0654	-	Update of SDP message content for test case 17.1	F	12.4.0	12.5.0	R5-150736
RP-67	RP-150322	0655	-	Correction to WI-103 Conference Call TC	F	12.4.0	12.5.0	R5-150745
RP-67	RP-150340	0656	-	Addition of new generic procedure for UE receiving SIP REFER request for transfer of additional CS to PS Call	F	12.4.0	12.5.0	R5-150931
RP-68	RP-150883	0658	-	Add GBA related abbreviations	F	12.5.0	12.6.0	R5-151112
RP-68	RP-150883	0660	-	Update of test case 15.14a	F	12.5.0	12.6.0	R5-151166
RP-68	RP-150883	0661	-	Update generic procedure C.21	F	12.5.0	12.6.0	R5-151183
RP-68	RP-150883	0663	-	Update generic procedure C.39	F	12.5.0	12.6.0	R5-151235
RP-68	RP-150883	0664	-	Update generic procedure C.40	F	12.5.0	12.6.0	R5-151236
RP-68	RP-150883	0666	-	Update REGISTER message with accesstype	F	12.5.0	12.6.0	R5-151242
RP-68	RP-150906	0668	-	Add new test case for MO speech / EVS	F	12.5.0	12.6.0	R5-151437
RP-68	RP-150883	0669	-	Editorial correction in generic procedure C.21	F	12.5.0	12.6.0	R5-151441
RP-68	RP-150886	0674	-	Update to test case 19.3.1 for location information	F	12.5.0	12.6.0	R5-151516
RP-68	RP-150886	0675	-	Update to test cases 19.1.1, 19.1.2, 19.3.3, 19.3.4, 19.4.1, 19.5.13.1 and Annex A.2.1 for location information	F	12.5.0	12.6.0	R5-151517
RP-68	RP-150886	0676	-	Correction to test case 19.1.3	F	12.5.0	12.6.0	R5-151519
RP-68	RP-150886	0677	-	Correction to test case 19.3.2	F	12.5.0	12.6.0	R5-151520
RP-68	RP-150886	0678	-	Correction to test case 19.3.2b	F	12.5.0	12.6.0	R5-151521
RP-68	RP-150886	0679	-	Correction to test case 19.3.2c	F	12.5.0	12.6.0	R5-151522
RP-68	RP-150883	0691	-	Correction for C.10 and C.38	F	12.5.0	12.6.0	R5-151681
RP-68	RP-150883	0694	-	Further corrections for SDP o-lines	F	12.5.0	12.6.0	R5-151684
RP-68	RP-150883	0704	-	Correction for test cases 15.21a and 15.21c	F	12.5.0	12.6.0	R5-151710
RP-68	RP-150883	0680	1	Correction to test cases 8.1, 8.10 and 8.11	F	12.5.0	12.6.0	R5-151794
RP-68	RP-150883	0657	1	Updates for GBA testing - Part1	F	12.5.0	12.6.0	R5-151795
RP-68	RP-150883	0662	1	Update generic procedure C.25	F	12.5.0	12.6.0	R5-151796
RP-68	RP-150883	0665	1	Update test case 15.21b	F	12.5.0	12.6.0	R5-151797
RP-68	RP-150883	0671	1	Correction to A.2.10 MO REFER Message	F	12.5.0	12.6.0	R5-151798
RP-68	RP-150883	0673	1	Correction to Annex Procedure C.28	F	12.5.0	12.6.0	R5-151799
RP-68	RP-150912	0683	1	Updates to Annex C.40	F	12.5.0	12.6.0	R5-151951
RP-68	RP-150883	0684	1	Correction and alignment of test cases 15.21 and 15.21b	F	12.5.0	12.6.0	R5-151952

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-68	RP-150883	0687	1	New TC 20.1 Mobile Originating CAT – Forking Model	F	12.5.0	12.6.0	R5-151953
RP-68	RP-150883	0692	1	Correction for C.19 and C.37	F	12.5.0	12.6.0	R5-151954
RP-68	RP-150883	0696	1	Correction of TC 17.2	F	12.5.0	12.6.0	R5-151956
RP-68	RP-150883	0697	1	Correction to C.31 and C.24	F	12.5.0	12.6.0	R5-151957
RP-68	RP-150883	0700	1	Correction to step number reference in 19.5.6, 19.5.8, 19.5.10	F	12.5.0	12.6.0	R5-151960
RP-68	RP-150883	0704	1	Corrections to TC 15.19	F	12.5.0	12.6.0	R5-151961
RP-68	RP-150906	0667	1	Add new generic procedure for MO speech / EVS	F	12.5.0	12.6.0	R5-151968
RP-68	RP-150883	0659	1	Correction to Annex Procedure C.25	F	12.5.0	12.6.0	R5-152091
RP-68	RP-150886	0690	1	Correction to IMS Emergency Call test case 19.4.2	F	12.5.0	12.6.0	R5-152092
RP-68	RP-150883	0701	1	References to default messages in C.10	F	12.5.0	12.6.0	R5-152093
RP-68	RP-150883	0703	1	Corrections to TC 18.1	F	12.5.0	12.6.0	R5-152094
RP-69	RP-151409	0707	-	Correction to 200 OK in C.28	F	12.6.0	12.7.0	R5-153202
RP-69	RP-151409	0710	-	Extending the registration expiration interval	F	12.6.0	12.7.0	R5-153254
RP-69	RP-151409	0711	-	Correction to Route header in MO INVITE	F	12.6.0	12.7.0	R5-153255
RP-69	RP-151409	0713	-	Corrections to TCs 15.27 and 15.28	F	12.6.0	12.7.0	R5-153258
RP-69	RP-151409	0715	-	Content-Type and Content-Length for 200 OK for other requests than REGISTER or SUBSCRIBE in case of SDP body	F	12.6.0	12.7.0	R5-153260
RP-69	RP-151409	0717	-	Correction of test case 15.21b	F	12.6.0	12.7.0	R5-153262
RP-69	RP-151409	0718	-	Editorial corrections	F	12.6.0	12.7.0	R5-153264
RP-69	RP-151409	0724	-	Correction to IMS authentication test case 9.1	F	12.6.0	12.7.0	R5-153463
RP-69	RP-151420	0725	-	Correction to Annex C.39 Generic test procedure for setting up MTSI MO speech call for rSRVCC	F	12.6.0	12.7.0	R5-153466
RP-69	RP-151411	0726	-	Correction to Emergency Service over IMS test case 19.3.1	F	12.6.0	12.7.0	R5-153472
RP-69	RP-151409	0728	-	Correction to WI-103 IMS Testcase 15.8	F	12.6.0	12.7.0	R5-153525
RP-69	RP-151427	0731	-	Add new test case for MT speech / EVS	F	12.6.0	12.7.0	R5-153535
RP-69	RP-151427	0733	-	Update test case 12.23	F	12.6.0	12.7.0	R5-153537
RP-69	RP-151411	0738	-	Adding note for Moving the MTSI SSAC access probability	F	12.6.0	12.7.0	R5-153593
RP-69	RP-151409	0739	-	Usage of “a=sendrecv” following deletion of “a=inactive”	F	12.6.0	12.7.0	R5-153610
RP-69	RP-151420	0705	1	Updates to generic test procedure C.43	F	12.6.0	12.7.0	R5-153754
RP-69	RP-151409	0706	1	Correction to generic test procedure C.24	F	12.6.0	12.7.0	R5-153755
RP-69	RP-151409	0708	1	Un-subscriptions before de-registrations	F	12.6.0	12.7.0	R5-153756
RP-69	RP-151409	0712	1	Editorial corrections to C.20	F	12.6.0	12.7.0	R5-153758
RP-69	RP-151409	0714	1	Further corrections for SDP o-lines	F	12.6.0	12.7.0	R5-153759
RP-69	RP-151409	0719	1	Clarifications to handle GRUU in SIP signalling	F	12.6.0	12.7.0	R5-153760
RP-69	RP-151409	0721	1	RSeq in 183 Session Progress	F	12.6.0	12.7.0	R5-153761
RP-69	RP-151409	0723	1	Corrections to option tags in Supported and Require header	F	12.6.0	12.7.0	R5-153762
RP-69	RP-151409	0727	1	Clarifications and corrections to IMS test case 20.1	F	12.6.0	12.7.0	R5-153763
RP-69	RP-151409	0729	1	Clarifications for A.6.2	F	12.6.0	12.7.0	R5-153764

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-69	RP-151409	0734	1	Correction to Annexes C.19 and C.37	F	12.6.0	12.7.0	R5-153765
RP-69	RP-151409	0736	1	Correction to video and smsip feature tags	F	12.6.0	12.7.0	R5-153766
RP-69	RP-151427	0730	1	Add new generic procedure for MT speech / EVS	F	12.6.0	12.7.0	R5-153798
RP-69	RP-151427	0741	1	Add new EVS test case 12.25 MO MTSI speech call / EVS / AMR-WB	F	12.6.0	12.7.0	R5-153950
RP-69	RP-151409	0709	1	Subscription to conf event: in-dialog or out-of-dialog?	F	12.6.0	12.7.0	R5-153986
RP-69	RP-151409	0716	1	Multiple tag-values in icsi-ref feature parameter	F	12.6.0	12.7.0	R5-153987
RP-69	RP-151411	0742	1	Correction to IMS Emergency Call test case 19.1.3	F	12.6.0	12.7.0	R5-153988
RP-69	RP-151409	0743	1	Split of XCAP test case 15.14a for communication barring while roaming	F	12.6.0	12.7.0	R5-153995
RP-69	RP-151427	0732	2	Correct annex C.44	F	12.6.0	12.7.0	R5-153999
RP-69	-	-	-	update of the "non-specific references" in section 2 according to the approved R5-153582 and an action point on ETSI MCC	-	12.6.0	12.7.0	-
RP-70	RP-151684	0744	-	Correction for pub-gruu and temp-gruu in A.1.6 NOTIFY	F	12.7.0	12.8.0	R5-155068
RP-70	RP-151684	0745	-	Correction for message body of NOTIFY at step 7 in C.19	F	12.7.0	12.8.0	R5-155069
RP-70	RP-151684	0751	-	Correction to test case 19.5.10	F	12.7.0	12.8.0	R5-155172
RP-70	RP-151684	0753	-	Correction to A.2.1 regarding lr parameter	F	12.7.0	12.8.0	R5-155174
RP-70	RP-151684	0754	-	Corrections to IMS test cases 19.3.3 and 19.3.4	F	12.7.0	12.8.0	R5-155175
RP-70	RP-151684	0756	-	Corrections to MMI command for Three Way Conferencing	F	12.7.0	12.8.0	R5-155177
RP-70	RP-151684	0757	-	Correction to Record-Route header in C.10	F	12.7.0	12.8.0	R5-155179
RP-70	RP-151684	0759	-	Removal of duplicated text in C.28	F	12.7.0	12.8.0	R5-155182
RP-70	RP-151684	0760	-	Correction to uniqueness of branch parameters	F	12.7.0	12.8.0	R5-155183
RP-70	RP-151684	0761	-	Update annex C.29.2 with BSF requirement	F	12.7.0	12.8.0	R5-155363
RP-70	RP-151703	0762	-	Editorial update of test case 12.23	F	12.7.0	12.8.0	R5-155458
RP-70	RP-151713	0776	-	Correction to Annex C.40	F	12.7.0	12.8.0	R5-155694
RP-70	RP-151684	0748	1	Corrections to the IMS Deregistration procedure	F	12.7.0	12.8.0	R5-155913
RP-70	RP-151684	0750	1	Corrections to IMS emergency test case 19.3.1	F	12.7.0	12.8.0	R5-155914
RP-70	RP-151684	0758	1	Referencing RFC 7315	F	12.7.0	12.8.0	R5-155915
RP-70	RP-151684	0773	1	Corrections to the use of the PUBLISH method	F	12.7.0	12.8.0	R5-155916
RP-70	RP-151703	0746	1	Editorial updates for EVS	F	12.7.0	12.8.0	R5-155918
RP-70	RP-151703	0763	1	Editorial update of test case 12.25	F	12.7.0	12.8.0	R5-155919
RP-70	RP-151703	0766	1	Add new test case for MT MTSI speech call / EVS / AMR-WB IO mode	F	12.7.0	12.8.0	R5-155920
RP-70	RP-151684	0774	2	Correction to Annex A regarding additional information	F	12.7.0	12.8.0	R5-155943
RP-70	RP-151684	0747	1	Update of P-Access-Network-Info header field in A.2.7 ACK	F	12.7.0	12.8.0	R5-155994
RP-70	RP-151684	0749	1	Corrections to IMS test case 15.29	F	12.7.0	12.8.0	R5-155995

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-70	RP-151684	0752	1	Clarification on usage of IR.92	F	12.7.0	12.8.0	R5-155997
RP-70	RP-151687	0764	1	Correction to IMS Emergency call test case 19.1.3	F	12.7.0	12.8.0	R5-155998
RP-70	RP-151684	0758	1	Correction of misplaced + another editorial correction of R5-155915	F	12.8.0	12.8.1	R5-155915
RP-71	RP-160096	0794	-	New Annex H definition for MTSI over Fixed Broadband Access	F	12.8.1	12.9.0	R5-160288
RP-71	RP-160096	0796	-	New Generic Registration Test Procedure for SIP Digest without TLS	F	12.8.1	12.9.0	R5-160290
RP-71	RP-160096	0798	-	New TC H.8.2 User Initiated Re-Registration / Fixed Broadband Access	F	12.8.1	12.9.0	R5-160292
RP-71	RP-160096	0799	-	New H.12.3 TC Originating MTSI Voice Call Successful with preconditions / Fixed Broadband Access	F	12.8.1	12.9.0	R5-160293
RP-71	RP-160097	0801	-	New Annex G definition for MTSI over WLAN	F	12.8.1	12.9.0	R5-160295
RP-71	RP-160119	0804	-	Removing Rel-9 SSAC test descriptions from 34.229-1	F	12.8.1	12.9.0	R5-160324
RP-71	RP-160130	0805	-	Removing Rel-12 SSAC test descriptions from 34.229-1	F	12.8.1	12.9.0	R5-160325
RP-71	RP-160117	0807	-	Clarification for conference media label used in NOTIFY for conference event package messages sent to the UE in C.19	F	12.8.1	12.9.0	R5-160435
RP-71	RP-160096	0808	-	Addition of new test case H.12.1 : Originating – 503 Service Unavailable / Fixed Broadband Access	F	12.8.1	12.9.0	R5-160505
RP-71	RP-160096	0809	-	Addition of new test case H.12.2 : Originating – 504 Server Time-out / Fixed Broadband Access	F	12.8.1	12.9.0	R5-160509
RP-71	RP-160117	0812	-	Expired grace period for video feature parameter and conference event subscription	F	12.8.1	12.9.0	R5-160553
RP-71	RP-160117	0821	-	Corrections to XML declarations	F	12.8.1	12.9.0	R5-160612
RP-71	RP-160117	0783	1	Update precondition requirements in C.11	F	12.8.1	12.9.0	R5-160790
RP-71	RP-160117	0785	1	Update precondition requirements in C.8	F	12.8.1	12.9.0	R5-160792
RP-71	RP-160117	0786	1	Update precondition requirements in C.9	F	12.8.1	12.9.0	R5-160793
RP-71	RP-160117	0787	1	Update test case 17.1	F	12.8.1	12.9.0	R5-160794
RP-71	RP-160117	0788	1	Update test case 17.2	F	12.8.1	12.9.0	R5-160795
RP-71	RP-160117	0790	1	Corrections to Conferencing test cases	F	12.8.1	12.9.0	R5-160796
RP-71	RP-160117	0791	1	Corrections to XCAP test cases	F	12.8.1	12.9.0	R5-160797
RP-71	RP-160119	0802	1	Corrections to IMS test case 19.5.1	F	12.8.1	12.9.0	R5-160798
RP-71	RP-160117	0810	1	Corrections to Authorization header in C.29.2	F	12.8.1	12.9.0	R5-160901
RP-71	RP-160117	0814	1	Update precondition requirements in C.13	F	12.8.1	12.9.0	R5-160903
RP-71	RP-160117	0815	1	Update precondition requirements in C.15	F	12.8.1	12.9.0	R5-160904
RP-71	RP-160117	0822	1	Corrections to RS and RR modifiers	F	12.8.1	12.9.0	R5-160906
RP-71	RP-160119	0825	1	Correction to IMS test case 19.1.3	F	12.8.1	12.9.0	R5-160907
RP-71	RP-160096	0793	1	New TC H.8.1 Initial registration / Fixed Broadband Access	F	12.8.1	12.9.0	R5-160913

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-71	RP-160096	0795	1	Correction to default IMS Registration messages for new Fixed Broadband Access Registration test cases	F	12.8.1	12.9.0	R5-160914
RP-71	RP-160096	0797	1	New Generic Test Procedure for MTSI Originating speech call over Fixed Broadband Access	F	12.8.1	12.9.0	R5-160915
RP-71	RP-160101	0782	1	Update precondition requirements in C.45	F	12.8.1	12.9.0	R5-160916
RP-71	RP-160101	0820	1	Update EVS requirements in test case 12.26	F	12.8.1	12.9.0	R5-160917
RP-71	RP-160101	0823	1	Update EVS requirements in C.44	F	12.8.1	12.9.0	R5-160918
RP-71	RP-160101	0824	1	Update EVS requirements in C.45	F	12.8.1	12.9.0	R5-160919
RP-71	RP-160119	0826	-	Correction to IMS emergency call test cases 19.3.2, 19.3.2b and 19.3.2c	F	12.8.1	12.9.0	R5-160937
RP-71	RP-160117	0811	1	Adding GSMA IR.94 reference	F	12.8.1	12.9.0	R5-160943
RP-71	RP-160117	0818	1	New test case 15.2a Originating Identification Restriction / Signalling	F	12.8.1	12.9.0	R5-160975
RP-71	RP-160117	0819	1	New test case 15.4a Terminating Identification Restriction / Signalling	F	12.8.1	12.9.0	R5-160976
RP-72	RP-160845	0827	-	Corrections to IMS test case 15.2a	F	12.9.0	12.10.0	R5-162034
RP-72	RP-160858	0834	-	Update test case 12.25	F	12.9.0	12.10.0	R5-162045
RP-72	RP-160858	0835	-	Update test case 12.26	F	12.9.0	12.10.0	R5-162046
RP-72	RP-160845	0838	-	Editorial correction of test case 15.4a	F	12.9.0	12.10.0	R5-162049
RP-72	RP-160845	0839	-	Correction of test case 18.1	F	12.9.0	12.10.0	R5-162050
RP-72	RP-160847	0840	-	Editorial correction of A.2.1, A.2.3, A.2.6, A.3.1	F	12.9.0	12.10.0	R5-162051
RP-72	RP-160845	0841	-	Corrections to Contact header of MO INVITE	F	12.9.0	12.10.0	R5-162054
RP-72	RP-160831	0843	-	Add test case for Originating Identification Restriction / WLAN	F	12.9.0	12.10.0	R5-162067
RP-72	RP-160831	0845	-	Add test case for Terminating Identification Restriction / WLAN	F	12.9.0	12.10.0	R5-162069
RP-72	RP-160830	0847	-	Add test case for Originating Identification Restriction / Fixed Broadband Access	F	12.9.0	12.10.0	R5-162103
RP-72	RP-160830	0849	-	Add test case for Terminating Identification Restriction / Fixed Broadband Access	F	12.9.0	12.10.0	R5-162105
RP-72	RP-160845	0851	-	Adding reference to RFC 3311	F	12.9.0	12.10.0	R5-162117
RP-72	RP-160845	0854	-	Correction to reference regarding GRUU reg event	F	12.9.0	12.10.0	R5-162129
RP-72	RP-160845	0855	-	Corrections to IMS test cases 15.10 and 15.13 regarding rule-deactivated	F	12.9.0	12.10.0	R5-162147
RP-72	RP-160845	0857	-	Corrections regarding security schemes and applicability	F	12.9.0	12.10.0	R5-162150
RP-72	RP-160830	0862	-	New H.12.5 TC Terminating MTSI Voice call with preconditions / Fixed Broadband Access	F	12.9.0	12.10.0	R5-162160
RP-72	RP-160830	0863	-	New H.8.3 TC User Initiated Deregistration / Fixed Broadband Access	F	12.9.0	12.10.0	R5-162161
RP-72	RP-160830	0866	-	TC H.8.1 Conformance Requirement update to include TS 24.229 Annex E Reference	F	12.9.0	12.10.0	R5-162506
RP-72	RP-160858	0867	-	Correction to Annex C.40	F	12.9.0	12.10.0	R5-162630

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-72	RP-160845	0870	-	Correction to Conference Facroty URI in Annex C.10 and C.38	F	12.9.0	12.10.0	R5-162721
RP-72	RP-160858	0828	1	Update precondition requirements in test case 12.25	F	12.9.0	12.10.0	R5-162925
RP-72	RP-160858	0829	1	Update precondition requirements in test case 12.26	F	12.9.0	12.10.0	R5-162926
RP-72	RP-160845	0830	1	Update precondition requirements in C.21	F	12.9.0	12.10.0	R5-162927
RP-72	RP-160858	0831	1	Update precondition requirements in C.44	F	12.9.0	12.10.0	R5-162928
RP-72	RP-160845	0832	1	Update precondition requirements in C.25	F	12.9.0	12.10.0	R5-162929
RP-72	RP-160845	0833	1	Update precondition requirements in C.26	F	12.9.0	12.10.0	R5-162930
RP-72	RP-160845	0836	1	Update test case 17.2	F	12.9.0	12.10.0	R5-162931
RP-72	RP-160845	0852	1	Corrections to IMS test case 20.1 regarding P-Early-Media header	F	12.9.0	12.10.0	R5-162934
RP-72	RP-160830	0871	-	Correction to C.21b regarding RS/RR modifiers	F	12.9.0	12.10.0	R5-162935
RP-72	RP-160847	0868	1	Correction to IMS test case 19.4.2	F	12.9.0	12.10.0	R5-162937
RP-72	RP-160830	0846	1	Add test case for Originating Identification Presentation / Fixed Broadband Access	F	12.9.0	12.10.0	R5-162943
RP-72	RP-160830	0848	1	Add test case for Terminating Identification Presentation / Fixed Broadband Access	F	12.9.0	12.10.0	R5-162944
RP-72	RP-160830	0858	1	Adding references to default IMS Registration messages for fixed Broadband Access	F	12.9.0	12.10.0	R5-162945
RP-72	RP-160830	0859	1	New conditions to Default messages for Call Setup for new fixed Broadband Access test cases	F	12.9.0	12.10.0	R5-162946
RP-72	RP-160831	0842	1	Add test case for Originating Identification Presentation / WLAN	F	12.9.0	12.10.0	R5-162947
RP-72	RP-160831	0844	1	Add test case for Terminating Identification Presentation / WLAN	F	12.9.0	12.10.0	R5-162948
RP-72	RP-160858	0873	-	Update of generic procedure C.45 for setting up MT speech call for EPS / EVS	F	12.9.0	12.10.0	R5-163042
RP-72	RP-160830	0860	1	New Generic Test Procedure for UE Initiated Deregistration for Fixed Broadband Access	F	12.9.0	12.10.0	R5-163087
RP-72	RP-160830	0861	1	New Generic Test Procedure for MTSI Terminating speech call over Fixed Broadband Access	F	12.9.0	12.10.0	R5-163088
RP-72	RP-160845	0850	2	Corrections to handling of conditions in Appendix A	F	12.9.0	12.10.0	R5-163199
RP-72	RP-160847	0872	1	Corrections to IMS test case 19.5.8	F	12.9.0	12.10.0	R5-163200
RP-72	RP-160845	0874	1	Addition of generic procedure for IMS re-registration	F	12.9.0	12.10.0	R5-163201
RP-73	RP-161428	0875	-	Corrections to IMS test case 19.4.2	F	12.10.0	12.11.0	R5-165040
RP-73	RP-161426	0876	-	Correction to precondition option tag in C.25	F	12.10.0	12.11.0	R5-165041
RP-73	RP-161426	0878	-	Correction to IMS test case 17.2	F	12.10.0	12.11.0	R5-165043
RP-73	RP-161426	0879	-	Add reference to RFC 6086	F	12.10.0	12.11.0	R5-165045
RP-73	RP-161426	0880	-	Corrections to strength tags in SDP	F	12.10.0	12.11.0	R5-165081
RP-73	RP-161426	0881	-	Corrections to usage of g.3gpp.state-and-event	F	12.10.0	12.11.0	R5-165086
RP-73	RP-161426	0883	-	Corrections to IMS test case 11.2	F	12.10.0	12.11.0	R5-165151

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-73	RP-161426	0892	-	Adding core spec reference for User-Agent field to C.29	F	12.10.0	12.11.0	R5-165195
RP-73	RP-161397	0894	-	Add test case for Communication Forwarding unconditional / WLAN	F	12.10.0	12.11.0	R5-165203
RP-73	RP-161397	0895	-	Add test case for Communication Forwarding on non Reply: activation / WLAN	F	12.10.0	12.11.0	R5-165204
RP-73	RP-161397	0896	-	Add test case for Communication Forwarding on non reply: MO call initiation / WLAN	F	12.10.0	12.11.0	R5-165205
RP-73	RP-161397	0897	-	Add test case for Communication Forwarding on Busy / WLAN	F	12.10.0	12.11.0	R5-165206
RP-73	RP-161397	0898	-	Add test case for Communication Forwarding on Not logged-in / WLAN	F	12.10.0	12.11.0	R5-165207
RP-73	RP-161397	0899	-	Add test case for Communication Forwarding on Not reachable / WLAN	F	12.10.0	12.11.0	R5-165208
RP-73	RP-161426	0900	-	Update test case 15.7	F	12.10.0	12.11.0	R5-165233
RP-73	RP-161426	0901	-	Update test case 15.10a	F	12.10.0	12.11.0	R5-165234
RP-73	RP-161396	0903	-	Add test case for Communication Forwarding unconditional / Fixed Broadband Access	F	12.10.0	12.11.0	R5-165285
RP-73	RP-161396	0904	-	Add test case for Communication Forwarding on non Reply: activation / Fixed Broadband Access	F	12.10.0	12.11.0	R5-165286
RP-73	RP-161396	0905	-	Add test case for Communication Forwarding on non reply: MO call initiation / Fixed Broadband Access	F	12.10.0	12.11.0	R5-165287
RP-73	RP-161396	0906	-	Add test case for Communication Forwarding on Busy / Fixed Broadband Access	F	12.10.0	12.11.0	R5-165288
RP-73	RP-161396	0907	-	Add test case for Communication Forwarding on Not logged-in / Fixed Broadband Access	F	12.10.0	12.11.0	R5-165289
RP-73	RP-161396	0908	-	Add test case for Communication Forwarding on Not reachable / Fixed Broadband Access	F	12.10.0	12.11.0	R5-165290
RP-73	RP-161426	0909	-	Cleanup of final conference URI	F	12.10.0	12.11.0	R5-165305
RP-73	RP-161426	0910	-	Corrections to IMS test case 9.1	F	12.10.0	12.11.0	R5-165323
RP-73	RP-161426	0911	-	Correction to test case 20.1	F	12.10.0	12.11.0	R5-165328
RP-73	RP-161426	0919	-	On usage of px_MessageServerDomainName	F	12.10.0	12.11.0	R5-165659
RP-73	RP-161426	0922	-	Correction to Structure of XML in Test Requirements for XCAP TCs.	F	12.10.0	12.11.0	R5-165883
RP-73	RP-161426	0893	1	Moving from RFC 3265 to RFC 6665	F	12.10.0	12.11.0	R5-165936
RP-73	RP-161428	0921	1	Correction to IMS emergency test case 19.5.1	F	12.10.0	12.11.0	R5-165938
RP-73	RP-161426	0913	1	Corrections to IMS test case 9.2	F	12.10.0	12.11.0	R5-165939
RP-73	RP-161438	0924	-	Correction to contents of REGISTER request message	F	12.10.0	12.11.0	R5-165940
RP-73	RP-161426	0916	1	Correction to pub GRUU and temp GRUU for TEL URI	F	12.10.0	12.11.0	R5-165941
RP-73	RP-161426	0918	1	Correction to IMS generic call establishment procedures for DTMF support	F	12.10.0	12.11.0	R5-165942
RP-73	RP-161396	0890	1	Update test case H.15.1	F	12.10.0	12.11.0	R5-165944
RP-73	RP-161396	0891	1	Update test case H.15.3	F	12.10.0	12.11.0	R5-165945

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-73	RP-161396	0920	1	Corrections and clarifications to Fixed Broadband default messages	F	12.10.0	12.11.0	R5-165946
RP-73	RP-161397	0885	1	Add test case for initial IMS registration / WLAN	F	12.10.0	12.11.0	R5-165947
RP-73	RP-161397	0886	1	Add test case for adding and removing video from MO Speech / WLAN	F	12.10.0	12.11.0	R5-165948
RP-73	RP-161397	0887	1	Add test case for adding and removing video from MT Speech / WLAN	F	12.10.0	12.11.0	R5-165949
RP-73	RP-161397	0888	1	Update test case G.15.1	F	12.10.0	12.11.0	R5-165950
RP-73	RP-161397	0889	1	Update test case G.15.3	F	12.10.0	12.11.0	R5-165951
RP-73	RP-161426	0902	1	Clarify GBA usage	F	12.10.0	12.11.0	R5-166279
RP-73	RP-161426	0917	1	Correction to A.2.1 condition regarding P-Early-Media header	F	12.10.0	12.11.0	R5-166280
RP-73	RP-161426	0923	1	Add audio tag requirements	F	12.11.0	13.0.0	R5-165943
RP-74	RP-162102	0925	-	Update AMR-WB requirements in C.21	F	13.0.0	13.1.0	R5-168031
RP-74	RP-162102	0926	-	Update AMR-WB requirements in C.25	F	13.0.0	13.1.0	R5-168032
RP-74	RP-162102	0927	-	Update AMR-WB requirements in C.28	F	13.0.0	13.1.0	R5-168033
RP-74	RP-162102	0928	-	Update AMR-WB requirements in C.31	F	13.0.0	13.1.0	R5-168034
RP-74	RP-162102	0929	-	Update AMR-WB requirements in C.39	F	13.0.0	13.1.0	R5-168053
RP-74	RP-162102	0930	-	Update AMR-WB requirements in C.40	F	13.0.0	13.1.0	R5-168054
RP-74	RP-162102	0931	-	Update AMR-WB requirements in C.43	F	13.0.0	13.1.0	R5-168055
RP-74	RP-162102	0933	-	Update AMR-WB requirements in C.11	F	13.0.0	13.1.0	R5-168057
RP-74	RP-162102	0934	-	Update AMR-WB requirements in C.26	F	13.0.0	13.1.0	R5-168058
RP-74	RP-162102	0935	-	Update AMR-WB requirements in C.42	F	13.0.0	13.1.0	R5-168059
RP-74	RP-162102	0955	-	Update AMR-WB requirements in test case 15.6	F	13.0.0	13.1.0	R5-168116
RP-74	RP-162102	0956	-	Update AMR-WB requirements in test case 15.21	F	13.0.0	13.1.0	R5-168117
RP-74	RP-162102	0957	-	Update AMR-WB requirements in test case 15.21b	F	13.0.0	13.1.0	R5-168119
RP-74	RP-162102	0958	-	Update AMR-WB requirements in test case 17.1	F	13.0.0	13.1.0	R5-168141
RP-74	RP-162102	0959	-	Update AMR-WB requirements in test case 17.2	F	13.0.0	13.1.0	R5-168142
RP-74	RP-162074	0960	-	Update C.29.1 for WLAN	F	13.0.0	13.1.0	R5-168143
RP-74	RP-162074	0961	-	Add test case for Incoming Communication Barring while roaming / WLAN	F	13.0.0	13.1.0	R5-168212
RP-74	RP-162074	0962	-	Add test case for Outgoing Communication Barring while roaming / WLAN	F	13.0.0	13.1.0	R5-168213
RP-74	RP-162074	0963	-	Editorial update of WLAN supplementary services test cases	F	13.0.0	13.1.0	R5-168233
RP-74	RP-162073	0968	-	New H.8.4 TC Invalid behaviour - 423 Interval too brief / Fixed Broadband Access	F	13.0.0	13.1.0	R5-168281
RP-74	RP-162073	0969	-	New H.8.5 TC User initiated re-registration - 423 Interval Too Brief / Fixed Broadband Access	F	13.0.0	13.1.0	R5-168282
RP-74	RP-162073	0970	-	New H.11.2 TC Network initiated re-authentication / Fixed Broadband Access	F	13.0.0	13.1.0	R5-168285

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-74	RP-162074	0971	-	Add test case for MO Call Hold without announcement / WLAN	F	13.0.0	13.1.0	R5-168321
RP-74	RP-162074	0972	-	Add test case for MT Call Hold without announcement / WLAN	F	13.0.0	13.1.0	R5-168322
RP-74	RP-162074	0973	-	Add test case for MO video Call Hold without announcement / WLAN	F	13.0.0	13.1.0	R5-168323
RP-74	RP-162074	0974	-	Add test case for MT video Call Hold without announcement / WLAN	F	13.0.0	13.1.0	R5-168324
RP-74	RP-162074	0975	-	Add test case for Subscription to the MWI event package / WLAN	F	13.0.0	13.1.0	R5-168325
RP-74	RP-162074	0976	-	Add test case for Inviting user to conference by sending a REFER request to the conference focus / WLAN	F	13.0.0	13.1.0	R5-168326
RP-74	RP-162074	0977	-	Add test case for Joining a conference after being invited to it / WLAN	F	13.0.0	13.1.0	R5-168327
RP-74	RP-162074	0978	-	Add test case for Three way session creation / WLAN	F	13.0.0	13.1.0	R5-168328
RP-74	RP-162074	0979	-	Add test case for Inviting user to conference by sending a REFER request to the conference focus for video / WLAN	F	13.0.0	13.1.0	R5-168329
RP-74	RP-162074	0980	-	Add test case for Joining a conference after being invited to it with video / WLAN	F	13.0.0	13.1.0	R5-168330
RP-74	RP-162074	0981	-	Add test case for Three way session creation for video / WLAN	F	13.0.0	13.1.0	R5-168331
RP-74	RP-162074	0982	-	Add test case for Communication Waiting and answering the call / WLAN	F	13.0.0	13.1.0	R5-168332
RP-74	RP-162075	0984	-	Update test cases G.15.2	F	13.0.0	13.1.0	R5-168334
RP-74	RP-162075	0985	-	Update test cases G.15.4	F	13.0.0	13.1.0	R5-168335
RP-74	RP-162075	0986	-	Update test cases G.15.7	F	13.0.0	13.1.0	R5-168336
RP-74	RP-162102	0998	-	Corrections to IMS test case 8.2	F	13.0.0	13.1.0	R5-168940
RP-74	RP-162102	0999	-	Corrections to IMS test case 8.3	F	13.0.0	13.1.0	R5-168941
RP-74	RP-162102	1000	-	Corrections to IMS test case 8.13	F	13.0.0	13.1.0	R5-168942
RP-74	RP-162073	1001	-	Corrections to IMS test case H.8.3	F	13.0.0	13.1.0	R5-168943
RP-74	RP-162102	1003	-	Clarifications and Corrections to IMS test case 15.2a	F	13.0.0	13.1.0	R5-168945
RP-74	RP-162102	1004	-	Clarifications and Corrections to IMS test case 15.4a	F	13.0.0	13.1.0	R5-168946
RP-74	RP-162102	1005	-	Corrections to IMS test case 15.15	F	13.0.0	13.1.0	R5-168947
RP-74	RP-162102	1006	-	Corrections to IMS test cases 15.19 and 15.19a	F	13.0.0	13.1.0	R5-168948
RP-74	RP-162102	1007	-	Corrections to Annex C.11	F	13.0.0	13.1.0	R5-168949
RP-74	RP-162102	1008	-	Corrections to IMS de-registration in C.30	F	13.0.0	13.1.0	R5-168950
RP-74	RP-162075	1010	-	Adding name to heading of section G.8	F	13.0.0	13.1.0	R5-168952
RP-74	RP-162075	1020	-	Adding name to heading of section G.17	F	13.0.0	13.1.0	R5-168953
RP-74	RP-162102	1012	-	Remove opaque field from Authentication-Info header	F	13.0.0	13.1.0	R5-168954
RP-74	RP-162102	1013	-	Corrections to References	F	13.0.0	13.1.0	R5-168955

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-74	RP-162102	1014	-	Replacing hardcoded XCAP password by prearranged password	F	13.0.0	13.1.0	R5-168956
RP-74	RP-162102	0987	1	Correction to generic procedure for adding a participant to a conference	F	13.0.0	13.1.0	R5-169054
RP-74	RP-162104	0995	1	Correction to GCF WI-154 IMS Emergency Call test cases 19.3.2, 19.3.2b, 19.3.2c	F	13.0.0	13.1.0	R5-169055
RP-74	RP-162102	1017	1	Corrections to TMPI handling in C.29.2	F	13.0.0	13.1.0	R5-169057
RP-74	RP-162073	0990	1	Addition of New Annex for MTSI over Fixed Line Test Case –Generic test procedure for setting up Terminating MTSI speech call over Fixed Broadband Access without preconditions	F	13.0.0	13.1.0	R5-169060
RP-74	RP-162073	0992	1	Addition of New MTSI over Fixed Line Test Case – H.12.4 Originating MTSI Voice Call Successful without preconditions / Fixed Broadband Access	F	13.0.0	13.1.0	R5-169061
RP-74	RP-162073	0993	1	Addition of New MTSI over Fixed Line Test Case – H.12.6 Terminating MTSI Voice call without preconditions / Fixed Broadband Access	F	13.0.0	13.1.0	R5-169062
RP-74	RP-162073	1011	1	Addition of New Annex for MTSI over Fixed Line Test Case –Generic test procedure for setting up Originating MTSI speech call over Fixed Broadband Access without preconditions	F	13.0.0	13.1.0	R5-169063
RP-74	RP-162075	1016	1	Add generic procedure for IMS registration / WLAN	F	13.0.0	13.1.0	R5-169064
RP-74	RP-162075	0983	1	Add test case for Communication Waiting and cancelling the call / WLAN	F	13.0.0	13.1.0	R5-169065
RP-74	RP-162074	0965	1	New Generic test procedure for setting up MTSI MO speech call for WLAN	F	13.0.0	13.1.0	R5-169066
RP-74	RP-162074	0964	1	New G.12.1 MO MTSI speech call / WLAN	F	13.0.0	13.1.0	R5-169067
RP-74	RP-162074	0966	1	New G.12.2 MT MTSI speech call / WLAN	F	13.0.0	13.1.0	R5-169068
RP-74	RP-162074	0967	1	New Generic test procedure for setting up MTSI MT speech call for WLAN	F	13.0.0	13.1.0	R5-169069
RP-74	RP-162075	0988	1	Introduction of MO MTSI Video call for WLAN: Test in Annex G and generic test procedure in Annex C	F	13.0.0	13.1.0	R5-169070
RP-74	RP-162075	0989	1	Introduction of MT MTSI Video call for WLAN: Test in Annex G and generic test procedure in Annex C	F	13.0.0	13.1.0	R5-169071
RP-74	RP-162104	1002	1	Corrections to IMS test case 19.5.7	F	13.0.0	13.1.0	R5-169121
RP-74	RP-162102	1018	1	Removing unwanted requirements on Content-Length	F	13.0.0	13.1.0	R5-169122
RP-74	RP-162102	1019	-	Correction to default contents for REGISTER message	F	13.0.0	13.1.0	R5-169130
RP-74	RP-162075	0994	1	Add test case for Emergency call with emergency registration / WLAN	F	13.0.0	13.1.0	R5-169153
RP-74	RP-162102	1009	1	Corrections to condition handling in Annex A	F	13.0.0	13.1.0	R5-169170
RP-75	RP-170107	1021	-	Deletions of applicability and ICS/IXIT statements	F	13.1.0	13.2.0	R5-170525
RP-75	RP-170066	1022	-	Deletions of applicability and ICS/IXIT statements	F	13.1.0	13.2.0	R5-170526
RP-75	RP-170108	1025	-	Corrections to IMS test 12.26	F	13.1.0	13.2.0	R5-170530
RP-75	RP-170095	1026	-	Expired grace period for audio feature parameter	F	13.1.0	13.2.0	R5-170564
RP-75	RP-170095	1028	-	De-implementation of R5-168949	F	13.1.0	13.2.0	R5-170610

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-75	RP-170095	1029	-	Adding optional port number to BSF server address	F	13.1.0	13.2.0	R5-170611
RP-75	RP-170095	1030	-	Resolving cross-references in C.29.1	F	13.1.0	13.2.0	R5-170612
RP-75	RP-170108	1034	-	Swapping br-send and br-recv in C.45	F	13.1.0	13.2.0	R5-170670
RP-75	RP-170108	1035	-	Strength-tag in C.45	F	13.1.0	13.2.0	R5-170671
RP-75	RP-170097	1036	-	Corrections to IMS test case 19.5.6	F	13.1.0	13.2.0	R5-170672
RP-75	RP-170066	1047	-	New Generic Test Procedure for Originating MTSI Video Call for Fixed Broadband Access	F	13.1.0	13.2.0	R5-170781
RP-75	RP-170066	1048	-	New Generic Test Procedure for Terminating MTSI Video Call over Fixed Broadband Access	F	13.1.0	13.2.0	R5-170782
RP-75	RP-170066	1056	-	Correction of Default messages for IMS Registration / Fixed Broadband Access	F	13.1.0	13.2.0	R5-170885
RP-75	RP-170095	1058	-	Content-Type in A.2.1	F	13.1.0	13.2.0	R5-170921
RP-75	RP-170066	1065	-	Editorial update of fixed broadband access supplementary services test cases	F	13.1.0	13.2.0	R5-171213
RP-75	RP-170066	1066	-	Update test cases H.15.2	F	13.1.0	13.2.0	R5-171258
RP-75	RP-170066	1067	-	Update test cases H.15.4	F	13.1.0	13.2.0	R5-171269
RP-75	RP-170066	1068	-	Update test cases H.15.7	F	13.1.0	13.2.0	R5-171286
RP-75	RP-170107	1023	1	Resolve EN in G.8.1	F	13.1.0	13.2.0	R5-171473
RP-75	RP-170095	1027	1	Correction to test case 17.1	F	13.1.0	13.2.0	R5-171474
RP-75	RP-170095	1032	1	Unify description of IMS Registration	F	13.1.0	13.2.0	R5-171475
RP-75	RP-170107	1037	1	Update generic procedure MO speech for WLAN	F	13.1.0	13.2.0	R5-171476
RP-75	RP-170107	1038	1	Update generic procedure MT speech for WLAN	F	13.1.0	13.2.0	R5-171477
RP-75	RP-170107	1039	1	Update generic procedure MO video call for WLAN	F	13.1.0	13.2.0	R5-171478
RP-75	RP-170097	1040	1	Addition of new TC 19.4.6 “Emergency call without emergency registration / Failure of registration / Rejected by 403(Forbidden)”	F	13.1.0	13.2.0	R5-171480
RP-75	RP-170097	1071	-	Addition of new TC 19.1.6 “Emergency call with emergency registration / Success / GIBA against a network with GIBA support only”	F	13.1.0	13.2.0	R5-171482
RP-75	RP-170097	1072	-	Addition of new TC 19.4.7 “Emergency call without emergency registration / Failure of registration / GIBA support only”	F	13.1.0	13.2.0	R5-171484
RP-75	RP-170108	1044	1	Correction to MO INVITE for SRVCC in prealerting phase	F	13.1.0	13.2.0	R5-171486
RP-75	RP-170107	1057	1	Corrections to WLAN MO and MT MTSI Video call message contents and procedures	F	13.1.0	13.2.0	R5-171488
RP-75	RP-170095	1060	1	Correction to IMS MT video call procedure	F	13.1.0	13.2.0	R5-171489
RP-75	RP-170097	1061	1	Correction to GCF WI-154 IMS Emergency Call test case 19.1.3	F	13.1.0	13.2.0	R5-171490
RP-75	RP-170095	1064	1	Correction to IMS Speech AMR test cases 16.2, 16.3 and 16.4 for DTMF support	F	13.1.0	13.2.0	R5-171491
RP-75	RP-170107	1070	1	Generic Test Procedure renumbering for MTSI over WLAN	F	13.1.0	13.2.0	R5-171492

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-75	RP-170066	1049	1	New TC H.9.1 SIP digest without TLS – abnormal procedures – 403 Forbidden / Fixed Broadband Access	F	13.1.0	13.2.0	R5-171495
RP-75	RP-170066	1050	1	New TC H.12.7 Originating MTSI Video call without preconditions / Fixed Broadband Access	F	13.1.0	13.2.0	R5-171496
RP-75	RP-170066	1051	1	New TC H.12.8 Terminating MTSI Video call without preconditions / Fixed Broadband Access	F	13.1.0	13.2.0	R5-171497
RP-75	RP-170066	1052	1	New TC H.15.11 Self-Configuration via SIP based procedure / Fixed Broadband Access	F	13.1.0	13.2.0	R5-171498
RP-75	RP-170066	1053	1	New TC H.17.1 Originating Voice, add video remove video / Fixed Broadband Access	F	13.1.0	13.2.0	R5-171499
RP-75	RP-170066	1054	1	New H.17.2 TC Terminating Voice, add video remove video / Fixed Broadband Access	F	13.1.0	13.2.0	R5-171500
RP-75	RP-170066	1063	1	Update C.29.1 for fixed broadband access	F	13.1.0	13.2.0	R5-171501
RP-75	RP-170095	1055	1	tel URI in Conferencing	F	13.1.0	13.2.0	R5-171510
RP-75	RP-170097	1042	1	Corrections to C.22	F	13.1.0	13.2.0	R5-171511
RP-75	RP-170097	1045	1	Correction to IMS Emergency registration test case 19.5.10	F	13.1.0	13.2.0	R5-171589
RP-75	RP-170107	1059	1	Updates to test case G.19.1	F	13.1.0	13.2.0	R5-171590
RP-76	RP-171365	1073		Removal of IMS test case 19.5.8	F	13.2.0	13.3.0	R5-172032
RP-76	RP-171365	1076		Corrections to IMS emergency with roaming test cases	F	13.2.0	13.3.0	R5-172067
RP-76	RP-171376	1077		Editorial correction to 183 Session Progress message in A.2.3	F	13.2.0	13.3.0	R5-172068
RP-76	RP-171376	1078		Correction to generic test procedure defined in Annex C.44	F	13.2.0	13.3.0	R5-172069
RP-76	RP-171363	1080		Small corrections to 17.1	F	13.2.0	13.3.0	R5-172104
RP-76	RP-171375	1081		Corrections to C.40	F	13.2.0	13.3.0	R5-172118
RP-76	RP-171376	1084		Correcting step reference in C.45	F	13.2.0	13.3.0	R5-172121
RP-76	RP-171375	1086		Re-removing EN in G.15.10.4	F	13.2.0	13.3.0	R5-172125
RP-76	RP-171363	1087		Aligning values for bandwidth modifier RR	F	13.2.0	13.3.0	R5-172126
RP-76	RP-171363	1093		More editorial corrections to C.20	F	13.2.0	13.3.0	R5-172294
RP-76	RP-171375	1094		Corrections to G.15.7	F	13.2.0	13.3.0	R5-172296
RP-76	RP-171365	1096		Correction to A.2.1 regarding Via header	F	13.2.0	13.3.0	R5-172412
RP-76	RP-171375	1099		Corrections to registration tests for MTSI over WLAN	F	13.2.0	13.3.0	R5-172421
RP-76	RP-171376	1100		Corrections to Fixed Access Originating test cases	F	13.2.0	13.3.0	R5-172423
RP-76	RP-171375	1082	1	Corrections to G.17.1	F	13.2.0	13.3.0	R5-172928
RP-76	RP-171375	1083	1	Corrections to G.17.2	F	13.2.0	13.3.0	R5-172929
RP-76	RP-171363	1088	1	Corrections to telephone-event in DL messages	F	13.2.0	13.3.0	R5-172930
RP-76	RP-171363	1089	1	Corrections to telephone-event in UL messages	F	13.2.0	13.3.0	R5-172931
RP-76	RP-171375	1090	1	Update annex C.11a and C.26a	F	13.2.0	13.3.0	R5-172932
RP-76	RP-171375	1091	1	Update test case G.12.1 and G.12.2	F	13.2.0	13.3.0	R5-172933

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-76	RP-171365	1098	1	Correction to A.2.8 regarding security headers	F	13.2.0	13.3.0	R5-172934
RP-76	RP-171365	1102	1	Corrections to IMS Emergency test case 19.4.1	F	13.2.0	13.3.0	R5-172935
RP-76	RP-171334	1092	1	Populating Annex I including new test cases I.8.1a-d	F	13.2.0	13.3.0	R5-172947
RP-76	RP-171363	1105		Corrections to audio feature tag and addition grace period	F	13.2.0	13.3.0	R5-173021
RP-76	RP-171365	1075	1	Corrections to GCF WI-154 IMS emergency test case 19.5.10	F	13.2.0	13.3.0	R5-173022
RP-76	RP-171363	1095	1	Add session timer requirement	F	13.2.0	13.3.0	R5-173024
RP-76	RP-171363	1085	1	Removing grace period from From and To headers	F	13.2.0	13.3.0	R5-173026
RP-77	RP-171660	1106	-	Add annex for UE category M1	F	13.3.0	13.4.0	R5-173532
RP-77	RP-171660	1108	-	Add generic procedure MT speech call for UE category M1	F	13.3.0	13.4.0	R5-173535
RP-77	RP-171660	1109	-	Add test case for MO MTSI speech call / UE category M1	F	13.3.0	13.4.0	R5-173536
RP-77	RP-171660	1110	-	Add test case for MT MTSI speech call / UE category M1	F	13.3.0	13.4.0	R5-173537
RP-77	RP-171660	1111	-	Add test case for Initial registration / UE category M1	F	13.3.0	13.4.0	R5-173538
RP-77	RP-171660	1112	-	Add supplementary services test cases for UE category M1	F	13.3.0	13.4.0	R5-173555
RP-77	RP-171698	1113	-	Update test case G.15.17	F	13.3.0	13.4.0	R5-173586
RP-77	RP-171698	1114	-	Editorial update of test case G.15.4	F	13.3.0	13.4.0	R5-173587
RP-77	RP-171698	1115	-	Editorial update of test case G.15.7	F	13.3.0	13.4.0	R5-173588
RP-77	RP-171688	1117	-	Corrections to PIXITs used	F	13.3.0	13.4.0	R5-173598
RP-77	RP-171688	1119	-	Corrections to A.2.3	F	13.3.0	13.4.0	R5-173600
RP-77	RP-171660	1121	-	Add emergency service test cases for UE category M1	F	13.3.0	13.4.0	R5-173605
RP-77	RP-171690	1123	-	Corrections to IMS test case 19.4.6	F	13.3.0	13.4.0	R5-173607
RP-77	RP-171690	1124	-	Corrections to IMS test case 19.4.7	F	13.3.0	13.4.0	R5-173608
RP-77	RP-171698	1128	-	Aligning telephone-event in C.40 and C.43	F	13.3.0	13.4.0	R5-173631
RP-77	RP-171699	1153	-	Editorial Corrections to Annex H	F	13.3.0	13.4.0	R5-173814
RP-77	RP-171699	1163	-	Correction to generic test procedure for setting up MTSI MT speech call for EPS / EVS in Annex C.45	F	13.3.0	13.4.0	R5-174050
RP-77	RP-171688	1164	-	Clerical corrections to rtpmap attributes	F	13.3.0	13.4.0	R5-174098
RP-77	RP-171688	1169	-	Corrections to Generic Test Procedure C.21	F	13.3.0	13.4.0	R5-174119
RP-77	RP-171660	1107	1	Add generic procedure MO speech call for UE category M1	F	13.3.0	13.4.0	R5-174483
RP-77	RP-171679	1149	1	Update to MO SIP INVITE message for eCall over IMS Release 14 related IEs	F	13.3.0	13.4.0	R5-174537
RP-77	RP-171698	1116	1	Correction to C.29.1 regarding XCAP over WLAN	F	13.3.0	13.4.0	R5-174542
RP-77	RP-171688	1118	1	Corrections to IMS test case 17.1	F	13.3.0	13.4.0	R5-174543
RP-77	RP-171688	1120	1	Removing Session-ID	F	13.3.0	13.4.0	R5-174544

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-77	RP-171690	1122	1	Corrections to A.1.1 and A.2.1 for sake of IMS test case 19.1.6	F	13.3.0	13.4.0	R5-174545
RP-77	RP-171688	1126	1	Removal of unneeded test cases	F	13.3.0	13.4.0	R5-174546
RP-77	RP-171699	1146	1	Corrections to test case H.9.1	F	13.3.0	13.4.0	R5-174547
RP-77	RP-171699	1166	1	Corrections to Generic Test Procedure C.21b	F	13.3.0	13.4.0	R5-174553
RP-77	RP-171699	1167	1	Corrections to Generic Test Procedure C.21c	F	13.3.0	13.4.0	R5-174554
RP-77	RP-171699	1173	1	Update to Annex C.11b (IMS/FBBA)	F	13.3.0	13.4.0	R5-174555
RP-77	RP-171699	1174	1	Update to Annex C.25b (IMS/FBBA)	F	13.3.0	13.4.0	R5-174556
RP-77	RP-171699	1175	1	Update to Annex C.26b (IMS/FBBA)	F	13.3.0	13.4.0	R5-174557
RP-77	RP-171698	1181	1	Correction to C.2c	F	13.3.0	13.4.0	R5-174558
RP-77	RP-171653	1131	1	Additional details for test case I.8.1a	F	13.3.0	13.4.0	R5-174682
RP-77	RP-171653	1132	1	Additional details for test case I.8.1b	F	13.3.0	13.4.0	R5-174683
RP-77	RP-171653	1133	1	Additional details for test case I.8.1c	F	13.3.0	13.4.0	R5-174684
RP-77	RP-171653	1134	1	Additional details for test case I.8.1d	F	13.3.0	13.4.0	R5-174685
RP-77	RP-171653	1135	1	New test case I.12.1a	F	13.3.0	13.4.0	R5-174686
RP-77	RP-171653	1136	1	New test case I.12.1b	F	13.3.0	13.4.0	R5-174687
RP-77	RP-171653	1137	1	New test case I.12.1c	F	13.3.0	13.4.0	R5-174688
RP-77	RP-171653	1138	1	New test case I.12.1d	F	13.3.0	13.4.0	R5-174689
RP-77	RP-171653	1139	1	New test case I.12.2a	F	13.3.0	13.4.0	R5-174690
RP-77	RP-171653	1140	1	New test case I.12.2b	F	13.3.0	13.4.0	R5-174691
RP-77	RP-171653	1141	1	New test case I.12.2c	F	13.3.0	13.4.0	R5-174692
RP-77	RP-171653	1142	1	New test case I.12.2d	F	13.3.0	13.4.0	R5-174693
RP-77	RP-171653	1144	1	Addition to References for RCC.07	F	13.3.0	13.4.0	R5-174694
RP-77	RP-171678	1152	-	Addition of RFC reference for eCall over IMS Release 14	F	13.4.0	14.0.0	R5-173776
RP-77	RP-171684	1182	-	Addition of new XML parameters defined in Rel-14 into TC 19.1.6, 19.4.6 and 19.4.7	F	13.4.0	14.0.0	R5-174442
RP-77	RP-171679	1150	1	Update to 200 OK message for eCall over IMS Release 14 related IEs	F	13.4.0	14.0.0	R5-174525
RP-77	RP-171679	1157	1	Addition of Generic Test Procedure for NG eCall setup and MSD update	F	13.4.0	14.0.0	R5-174526
RP-77	RP-171679	1160	1	Addition of the new eCall over IMS Test Case- eCall over IMS / Manual initiation / Normal registration / Emergency registration / Success / 200 OK with ACK	F	13.4.0	14.0.0	R5-174527
RP-77	RP-171679	1168	1	Addition of the new eCall over IMS Test Case- eCall over IMS / Automatic initiation / Normal registration / Emergency registration / Success / 200 OK with ACK	F	13.4.0	14.0.0	R5-174529
RP-77	RP-171679	1170	1	eCall over IMS / Manual initiation / MSD transfer and 200 OK with ACK / SIP INFO request for MSD Update / Success	F	13.4.0	14.0.0	R5-174530

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-77	RP-171679	1172	1	Add INFO message for MO and MT for eCall over IMS	F	13.4.0	14.0.0	R5-174531
RP-77	RP-171679	1177	1	Addition of new IMS NG eCall test case 21.13 - eCall only mode / Manual initiation / Emergency registration / Abnormal case / IM CN sends a 486 (Busy Here) / UE performs eCall in CS domain / UTRAN or GERAN	F	13.4.0	14.0.0	R5-174533
RP-77	RP-171679	1178	1	Addition of new IMS NG eCall test case 21.15 - eCall only mode / Manual initiation / Emergency registration / Abnormal case / IM CN sends a 600 (Busy Everywhere) / UE performs eCall in CS domain / UTRAN or GERAN	F	13.4.0	14.0.0	R5-174534
RP-77	RP-171679	1179	1	Addition of new IMS NG eCall test case 21.16 - eCall only mode / Automatic initiation / Emergency registration / Abnormal case / IM CN sends a 600 (Busy Everywhere) / UE performs eCall in CS domain / UTRAN or GERAN	F	13.4.0	14.0.0	R5-174535
RP-77	RP-171679	1180	1	Addition of new IMS NG eCall test case 21.14 - eCall only mode / Automatic initiation / Emergency registration / Abnormal case / IM CN sends a 486 (Busy Here) / UE performs eCall in CS domain / UTRAN or GERAN	F	13.4.0	14.0.0	R5-174536
RP-78	RP-172217	1184	-	Addition of the new eCall over IMS Test Case 21.17	F	14.0.0	14.1.0	R5-176071
RP-78	RP-172217	1185	-	Addition of the new eCall over IMS Test Case 21.18	F	14.0.0	14.1.0	R5-176072
RP-78	RP-172217	1186	-	Update to IMS eCall test case 21.1	F	14.0.0	14.1.0	R5-176124
RP-78	RP-172217	1187	-	Update to IMS eCall test case 21.2	F	14.0.0	14.1.0	R5-176125
RP-78	RP-172217	1188	-	Update to IMS eCall test case 21.4	F	14.0.0	14.1.0	R5-176126
RP-78	RP-172217	1189	-	Update to IMS eCall test case 21.13	F	14.0.0	14.1.0	R5-176127
RP-78	RP-172217	1190	-	Update to IMS eCall test case 21.14	F	14.0.0	14.1.0	R5-176128
RP-78	RP-172217	1191	-	Update to IMS eCall test case 21.15	F	14.0.0	14.1.0	R5-176129
RP-78	RP-172217	1192	-	Update to IMS eCall test case 21.16	F	14.0.0	14.1.0	R5-176130
RP-78	RP-172236	1195	-	Update to WLAN test case G.15.7	F	14.0.0	14.1.0	R5-176158
RP-78	RP-172236	1196	-	Update to WLAN test case G.15.24	F	14.0.0	14.1.0	R5-176159
RP-78	RP-172236	1197	-	Update to WLAN test case G.15.25	F	14.0.0	14.1.0	R5-176160
RP-78	RP-172236	1198	-	Update to WLAN test case G.17.1	F	14.0.0	14.1.0	R5-176161
RP-78	RP-172237	1201	-	Update to FBBA test case H.15.7	F	14.0.0	14.1.0	R5-176164
RP-78	RP-172237	1202	-	Update to FBBA test case H.17.1	F	14.0.0	14.1.0	R5-176165
RP-78	RP-172237	1203	-	Update to FBBA test case H.17.2	F	14.0.0	14.1.0	R5-176166
RP-78	RP-172236	1205	-	Correction of WLAN Conference test procedures	F	14.0.0	14.1.0	R5-176168
RP-78	RP-172237	1206	-	Update to FBBA annex C.26b	F	14.0.0	14.1.0	R5-176169
RP-78	RP-172217	1208	-	eCall over IMS / Automatic initiation / MSD transfer and 200 OK with ACK / SIP INFO request for MSD Update / Success	F	14.0.0	14.1.0	R5-176178
RP-78	RP-172217	1210	-	Corrections to INFO requests for eCall over IMS	F	14.0.0	14.1.0	R5-176200
RP-78	RP-172217	1211	-	Corrections to A.3.1 200 OK for sake of eCall over IMS	F	14.0.0	14.1.0	R5-176201

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-78	RP-172217	1212	-	486 (Busy Here) response for eCall over IMS	F	14.0.0	14.1.0	R5-176202
RP-78	RP-172217	1213	-	600 (Busy Everywhere) response for eCall over IMS	F	14.0.0	14.1.0	R5-176203
RP-78	RP-172217	1214	-	603 (Decline) response for eCall over IMS	F	14.0.0	14.1.0	R5-176204
RP-78	RP-172235	1217	-	Corrections to usage of SRVCC alerting feature tag for video calls	F	14.0.0	14.1.0	R5-176209
RP-78	RP-172233	1219	-	Corrections to C.38	F	14.0.0	14.1.0	R5-176212
RP-78	RP-172233	1220	-	Corrections to C.21a and C.44 regarding bandwidth value RR	F	14.0.0	14.1.0	R5-176213
RP-78	RP-172197	1223	-	Removing feature tags for Converged IP Communications again	F	14.0.0	14.1.0	R5-176217
RP-78	RP-172197	1225	-	Corrections to I.8.1b	F	14.0.0	14.1.0	R5-176219
RP-78	RP-172197	1227	-	Additions and Corrections to I.8.1d	F	14.0.0	14.1.0	R5-176222
RP-78	RP-172197	1228	-	Additions and corrections to I.12	F	14.0.0	14.1.0	R5-176224
RP-78	RP-172238	1229	-	Update to CatM1 annex C.11d	F	14.0.0	14.1.0	R5-176226
RP-78	RP-172233	1231	-	Corrections to usage of video feature tag	F	14.0.0	14.1.0	R5-176371
RP-78	RP-172236	1199	1	Update to WLAN test case G.17.2	F	14.0.0	14.1.0	R5-176931
RP-78	RP-172237	1200	1	Update to FBBA annex C.11b	F	14.0.0	14.1.0	R5-176932
RP-78	RP-172233	1194	1	Update to test case 17.1	F	14.0.0	14.1.0	R5-176933
RP-78	RP-172234	1215	1	Extending timer tolerance in IMS test case 19.5.7	F	14.0.0	14.1.0	R5-176934
RP-78	RP-172233	1216	1	Correction to NOTE 4 in A.1.1	F	14.0.0	14.1.0	R5-176935
RP-78	RP-172233	1222	1	Corrections to Conferencing regarding end of participation	F	14.0.0	14.1.0	R5-176937
RP-78	RP-172233	1232	1	Corrections to C.30	F	14.0.0	14.1.0	R5-176939
RP-78	RP-172197	1226	1	Additions and Corrections to I.8.1c	F	14.0.0	14.1.0	R5-176945
RP-78	RP-172197	1224	1	Additions to I.8.1a	F	14.0.0	14.1.0	R5-176946
RP-78	RP-172217	1207	1	eCall over IMS / Manual initiation / MSD transfer Failure / UE performs eCall in CS domain after Timer expiry / UTRAN or GERAN	F	14.0.0	14.1.0	R5-176947
RP-78	RP-172217	1218	1	Corrections to A.2.1 INVITE for eCall	F	14.0.0	14.1.0	R5-176948
RP-78	RP-172217	1237	1	Addition of USIM settings for IMS eCall	F	14.0.0	14.1.0	R5-176949
RP-78	RP-172236	1239	1	Adding Content headers to 180 Ringing	F	14.0.0	14.1.0	R5-177068
RP-78	RP-172217	1241	-	Addition of new IMS eCall test case 21.6	F	14.0.0	14.1.0	R5-177070
RP-78	RP-172233	1221	2	Corrections regarding sess-version	F	14.0.0	14.1.0	R5-177121
RP-78	RP-172234	1240	1	Correction to IMS Test Cases 19.4.5, 19.4.6 and 19.4.7	F	14.0.0	14.1.0	R5-177122
RP-78	RP-172234	1242	-	Addition of Generic Test Procedures C.32a	F	14.0.0	14.1.0	R5-177124
RP-78	RP-172233	1230	2	Make audio feature tag dependent on dedicated PICS	F	14.0.0	14.1.0	R5-177127
RP-79	RP-180109	1244	-	Editorial update of headers for UE category M1 test cases	F	14.1.0	14.2.0	R5-180229
RP-79	RP-180104	1245	-	Expired grace period for session timer requirement	F	14.1.0	14.2.0	R5-180230

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-79	RP-180104	1246	-	Update audio media requirements	F	14.1.0	14.2.0	R5-180231
RP-79	RP-180104	1248	-	Corrections to Communication Forwarding on non reply regarding codec usage	F	14.1.0	14.2.0	R5-180327
RP-79	RP-180104	1250	-	Fixing step numbering of generic function being used in 17.2	F	14.1.0	14.2.0	R5-180431
RP-79	RP-180105	1251	-	Correction to IMS test case 19.4.7 regarding port in Record-Route header	F	14.1.0	14.2.0	R5-180433
RP-79	RP-180104	1252	-	Corrections to Conferencing test cases	F	14.1.0	14.2.0	R5-180434
RP-79	RP-180107	1254	-	Corrections to Converged IP Communications test case I.8.1d	F	14.1.0	14.2.0	R5-180483
RP-79	RP-180105	1255	-	Corrections to 19.4.5	F	14.1.0	14.2.0	R5-180492
RP-79	RP-180109	1256	-	Fixing cross reference for audio media feature tag	F	14.1.0	14.2.0	R5-180494
RP-79	RP-180104	1257	-	Clarification to A.3.1 regarding the Contact header	F	14.1.0	14.2.0	R5-180507
RP-79	RP-180107	1258	-	Corrections to G.8.1	F	14.1.0	14.2.0	R5-180512
RP-79	RP-180108	1261	-	Update to FBBA test case H.17.1	F	14.1.0	14.2.0	R5-180631
RP-79	RP-180089	1262	-	Updates to IMS eCall test cases	F	14.1.0	14.2.0	R5-180676
RP-79	RP-180105	1267	-	Resubmission of missed Addition of Generic Test Procedure C.32a	F	14.1.0	14.2.0	R5-180782
RP-79	RP-180104	1249	1	Corrections to Rseq header in 180 Ringing	F	14.1.0	14.2.0	R5-181190
RP-79	RP-180104	1253	1	Corrections to Converged IP Communications test cases I.8.1a and I.8.1b	F	14.1.0	14.2.0	R5-181191
RP-79	RP-180107	1260	1	Updates to test case G.19	F	14.1.0	14.2.0	R5-181192
RP-79	RP-180105	1269	1	Correction to XML body of A.4.1	F	14.1.0	14.2.0	R5-181193
RP-79	RP-180089	1259	1	Updates to default USIM settings for IMS eCall test cases	F	14.1.0	14.2.0	R5-181194
RP-79	RP-180107	1265	1	Update of Annex C.11a Generic procedure for WLAN MTSI MT speech call	F	14.1.0	14.2.0	R5-181313
RP-79	RP-180107	1266	1	Update of Annex C.26a Generic procedure for WLAN MTSI MT video call	F	14.1.0	14.2.0	R5-181314
RP-80	RP-180720	1270	1	Corrections to IMS test case 15.25	F	14.2.0	14.3.0	R5-182184
RP-80	RP-180720	1272	1	Usage of “a=sendrecv” and “a=inactive”: Revisited	F	14.2.0	14.3.0	R5-182188
RP-80	RP-180720	1276	-	Corrections to A.2.10 MO REFER	F	14.2.0	14.3.0	R5-182192
RP-80	RP-180725	1281	-	Correction of C.21, C.21a, C.21d	F	14.2.0	14.3.0	R5-182305
RP-80	RP-180723	1282	-	Corrections to step numberings in test cases for IMS over WLAN	F	14.2.0	14.3.0	R5-182352
RP-80	RP-180721	1283	-	Corrections to IMS emergency calls without registration	F	14.2.0	14.3.0	R5-182368
RP-80	RP-180721	1284	-	Correction to IMS emergency call test case 19.1.3	F	14.2.0	14.3.0	R5-182560
RP-80	RP-180723	1285	-	Update Annex A.2.1 with conditon A5 Re-Invite for pre-alerting Contact-Header feature-param	F	14.2.0	14.3.0	R5-182793
RP-80	RP-180723	1273	2	Corrections to C.26a	F	14.2.0	14.3.0	R5-183095
RP-80	RP-180726	1274	2	Corrections to IMS test case G.19.1	F	14.2.0	14.3.0	R5-183096

Meeting-1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-80	RP-180720	1275	2	Port 0 when removing a stream from a session	F	14.2.0	14.3.0	R5-183097
RP-80	RP-180723	1277	1	Corrections to C.11a	F	14.2.0	14.3.0	R5-183098
RP-80	RP-180721	1279	1	Update to test case 19.3.2c	F	14.2.0	14.3.0	R5-183099
RP-80	RP-180726	1280	1	Updates to several IMS eCall test cases	F	14.2.0	14.3.0	R5-183100
RP-80	RP-180721	1286	-	Correction to IMS emergency call test cases for IMS Reregistration over UTRAN	F	14.2.0	14.3.0	R5-183106
RP-80	RP-180725	1287	-	Addition of IMS test cases J.18.1 and J.18.2	F	14.2.0	14.3.0	R5-183107
RP-81	RP-181580	1288	-	Corrections to G.15.4	F	14.3.0	14.4.0	R5-184056
RP-81	RP-181578	1289	-	Resubmission of Corrections to IMS test case 19.1.6	F	14.3.0	14.4.0	R5-184062
RP-81	RP-181578	1290	-	Editorial corrections to IMS emergency call test cases in clauses 19 and 21	F	14.3.0	14.4.0	R5-184096
RP-81	RP-181582	1291	-	Add and use reference to NG.108	F	14.3.0	14.4.0	R5-184483
RP-81	RP-181583	1292	-	Update to IMS eCall test cases for eCall category bit usage	F	14.3.0	14.4.0	R5-184704
RP-81	RP-181578	1293	1	Update to Emergency Call test case 19.1.3 for eCall category bit usage	F	14.3.0	14.4.0	R5-185087
RP-82	RP-182283	1298	-	Corrections to IMS test case 15.25	F	14.4.0	14.5.0	R5-186459
RP-82	RP-182283	1299	-	Correction to Contact header in MT INVITE	F	14.4.0	14.5.0	R5-187374
RP-82	RP-182286	1300	-	Corrections to IMS WLAN test case G.17.2	F	14.4.0	14.5.0	R5-187567
RP-82	RP-182284	1297	1	Corrections to C.32 and C.32a	F	14.4.0	14.5.0	R5-187683
RP-83	RP-190091	1305	-	Corrections to 200 OK for "video" media feature tag	F	14.5.0	14.6.0	R5-191117
RP-83	RP-190091	1306	-	Further corrections to A.2.1 for sake of IMS test case 19.1.6	F	14.5.0	14.6.0	R5-191118
RP-83	RP-190091	1317	-	Editorial Corrections to A.2.1	F	14.5.0	14.6.0	R5-191216
RP-83	RP-190091	1301	1	Expired grace period for media parameters requirement	F	14.5.0	14.6.0	R5-192309
RP-83	RP-190097	1302	1	Update to A.2.1 for Test eCall Request-URI	F	14.5.0	14.6.0	R5-192310
RP-83	RP-190091	1304	1	Corrections to XCAP test cases regarding rule elements	F	14.5.0	14.6.0	R5-192311
RP-83	RP-190091	1307	1	New test case 22.1 for Session Timer: UE is able to refresh the session in MO Call	F	14.5.0	14.6.0	R5-192312
RP-83	RP-190091	1308	1	New test case 22.2 for Session Timer: Remote end is refresher in MO Call	F	14.5.0	14.6.0	R5-192313
RP-83	RP-190091	1309	1	New test case 22.3 for Session Timer: Remote end does not support Session Timer in MO Call	F	14.5.0	14.6.0	R5-192314
RP-83	RP-190091	1310	1	New test case 22.4 for Session Timer: Remote end supports but does not use Session Timer in MO Call	F	14.5.0	14.6.0	R5-192315
RP-83	RP-190091	1311	1	New test case 22.5 for Session Timer: Remote end supports but does not send Session-Expires in MT Call	F	14.5.0	14.6.0	R5-192316
RP-83	RP-190091	1312	1	New test case 22.6 for Session Timer: Remote end sends Session-Expires but does not choose refresher in MT Call	F	14.5.0	14.6.0	R5-192317

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-83	RP-190091	1313	1	New test case 22.7 for Session Timer: Remote end chooses UE as refresher in MT Call	F	14.5.0	14.6.0	R5-192318
RP-83	RP-190091	1314	1	New test case 22.8 for Session Timer: Remote end does not support Session Timer in MT Call	F	14.5.0	14.6.0	R5-192319
RP-83	RP-190091	1315	1	New clause A.2.24 for "422 Session Interval Too Small" error message	F	14.5.0	14.6.0	R5-192320
RP-83	RP-190091	1316	1	Corrections to INVITE regarding Session Timer	F	14.5.0	14.6.0	R5-192321
RP-83	RP-190095	1318	1	Adding TC 15.30 for user initiated USSI	F	14.5.0	14.6.0	R5-192322
RP-83	RP-190091	1319	1	Adding TC 12.13a for MT MTSI speech call when MO reserves resources before sending INVITE	F	14.5.0	14.6.0	R5-192323
RP-84	RP-190887	1320	-	A.1.1 table clean-up	F	14.6.0	14.7.0	R5-193845
RP-84	RP-190887	1322	-	A.3.1 table clean-up	F	14.6.0	14.7.0	R5-193850
RP-84	RP-190887	1325	-	Removal of Editor Notes from IMS test cases 16.2 and 16.3	F	14.6.0	14.7.0	R5-193854
RP-84	RP-190887	1321	1	A.2.1 table clean-up	F	14.6.0	14.7.0	R5-194825
RP-84	RP-190887	1323	1	Correcting clause headings in Appendix C	F	14.6.0	14.7.0	R5-194826
RP-84	RP-190887	1327	1	Extending scope of test case 15.2a	F	14.6.0	14.7.0	R5-194827
RP-84	RP-190887	1328	1	Addition of new MO MTSI Voice call scenario without pre-condition	F	14.6.0	14.7.0	R5-194829
RP-84	RP-190887	1329	1	Addition of new MT MTSI Voice call scenario without pre-condition	F	14.6.0	14.7.0	R5-194830
RP-84	RP-190891	1334	1	Corrections to bit-rate and bandwidth parameters in EVS	F	14.6.0	14.7.0	R5-195318
RP-84	RP-190868	1324	-	Adaptations of P-Access-Network-Info header usage for NR	F	14.7.0	15.0.0	R5-193853
RP-84	RP-190868	1326	1	Adaptations to generic text for IMS Registration for 5G	F	14.7.0	15.0.0	R5-195233
RP-84	RP-190868	1331	1	Generic procedure for MO voice call over NR	F	14.7.0	15.0.0	R5-195234
RP-84	RP-190868	1332	1	Adaptations to generic text for IMS Emergency Registration for 5G	F	14.7.0	15.0.0	R5-195235
RP-84	RP-190868	1335	-	Adaptations to generic text for IMS Emergency Speech Call for 5G	F	14.7.0	15.0.0	R5-195237
RP-85	RP-191704	1336	-	Clean-up of Annex A.1.1	F	15.0.0	15.1.0	R5-195811
RP-85	RP-191704	1337	-	Clean-up of Annex A.1.2	F	15.0.0	15.1.0	R5-195812
RP-85	RP-191704	1338	-	Clean-up of Annex A.1.3	F	15.0.0	15.1.0	R5-195813
RP-85	RP-191704	1339	-	Clean-up of Annex A.1.4	F	15.0.0	15.1.0	R5-195814
RP-85	RP-191704	1340	-	Clean-up of Annex A.1.5	F	15.0.0	15.1.0	R5-195815
RP-85	RP-191704	1341	-	Clean-up of Annex A.1.6	F	15.0.0	15.1.0	R5-195816
RP-85	RP-191704	1342	-	Clean-up of Annex A.1.7	F	15.0.0	15.1.0	R5-195817
RP-85	RP-191704	1343	-	Clean-up of Annex A.1.8	F	15.0.0	15.1.0	R5-195818

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-85	RP-191704	1344	-	Clean-up of Annex A.2.2	F	15.0.0	15.1.0	R5-195819
RP-85	RP-191704	1345	-	Clean-up of Annex A.2.3	F	15.0.0	15.1.0	R5-195820
RP-85	RP-191704	1346	-	Clean-up of Annex A.2.4	F	15.0.0	15.1.0	R5-195830
RP-85	RP-191704	1347	-	Clean-up of Annex A.2.5	F	15.0.0	15.1.0	R5-195832
RP-85	RP-191704	1348	-	Clean-up of Annex A.2.6	F	15.0.0	15.1.0	R5-195833
RP-85	RP-191704	1349	-	Clean-up of Annex A.2.7	F	15.0.0	15.1.0	R5-195835
RP-85	RP-191704	1350	-	Clean-up of Annex A.2.8	F	15.0.0	15.1.0	R5-195836
RP-85	RP-191704	1351	-	Clean-up of Annex A.2.9	F	15.0.0	15.1.0	R5-195837
RP-85	RP-191704	1352	-	Clean-up of Annex A.3.1	F	15.0.0	15.1.0	R5-195838
RP-85	RP-191704	1353	-	Clean-up of Annex A.3.2	F	15.0.0	15.1.0	R5-195839
RP-85	RP-191704	1354	-	Clean-up of Annex A.3.3	F	15.0.0	15.1.0	R5-195841
RP-85	RP-191704	1355	-	Clean-up of Annex A.2.10	F	15.0.0	15.1.0	R5-195842
RP-85	RP-191704	1356	-	Clean-up of Annex A.2.11	F	15.0.0	15.1.0	R5-195844
RP-85	RP-191704	1357	-	Clean-up of Annex A.2.12	F	15.0.0	15.1.0	R5-195845
RP-85	RP-191704	1358	-	Clean-up of Annex A.2.13	F	15.0.0	15.1.0	R5-195848
RP-85	RP-191704	1359	-	Clean-up of Annex A.2.14	F	15.0.0	15.1.0	R5-195851
RP-85	RP-191704	1360	-	Clean-up of Annex A.2.15	F	15.0.0	15.1.0	R5-195853
RP-85	RP-191704	1362	-	Clean-up of Annex A.2.17	F	15.0.0	15.1.0	R5-195855
RP-85	RP-191704	1363	-	Clean-up of Annex A.2.18	F	15.0.0	15.1.0	R5-195856
RP-85	RP-191704	1364	-	Clean-up of Annex A.2.19	F	15.0.0	15.1.0	R5-195857
RP-85	RP-191704	1365	-	Clean-up of Annex A.2.20	F	15.0.0	15.1.0	R5-195858
RP-85	RP-191704	1366	-	Clean-up of Annex A.2.21	F	15.0.0	15.1.0	R5-195859
RP-85	RP-191704	1367	-	Clean-up of Annex A.2.22	F	15.0.0	15.1.0	R5-195860
RP-85	RP-191704	1368	-	Clean-up of Annex A.2.23	F	15.0.0	15.1.0	R5-195861
RP-85	RP-191704	1369	-	Clean-up of Annex A.2.24	F	15.0.0	15.1.0	R5-195862
RP-85	RP-191704	1370	-	Clean-up of Annex A.4.1	F	15.0.0	15.1.0	R5-195863
RP-85	RP-191704	1371	-	Clean-up of Annex A.4.2	F	15.0.0	15.1.0	R5-195864
RP-85	RP-191704	1372	-	Clean-up of Annex A.4.3	F	15.0.0	15.1.0	R5-195866
RP-85	RP-191704	1373	-	Clean-up of Annex A.4.4	F	15.0.0	15.1.0	R5-195867

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-85	RP-191704	1374	-	Clean-up of Annex A.4.5	F	15.0.0	15.1.0	R5-195868
RP-85	RP-191704	1375	-	Clean-up of Annex A.4.6	F	15.0.0	15.1.0	R5-195869
RP-85	RP-191704	1376	-	Clean-up of Annex A.5.1	F	15.0.0	15.1.0	R5-195870
RP-85	RP-191704	1377	-	Clean-up of Annex A.5.2	F	15.0.0	15.1.0	R5-195871
RP-85	RP-191704	1378	-	Clean-up of Annex A.5.3	F	15.0.0	15.1.0	R5-195872
RP-85	RP-191704	1379	-	Clean-up of Annex A.6.1	F	15.0.0	15.1.0	R5-195873
RP-85	RP-191704	1380	-	Clean-up of Annex A.6.2	F	15.0.0	15.1.0	R5-195874
RP-85	RP-191704	1381	-	Clean-up of Annex A.6.3	F	15.0.0	15.1.0	R5-195875
RP-85	RP-191704	1382	-	Clean-up of Annex A.7.1	F	15.0.0	15.1.0	R5-195876
RP-85	RP-191704	1383	-	Clean-up of Annex A.7.2	F	15.0.0	15.1.0	R5-195877
RP-85	RP-191704	1384	-	Clean-up of Annex A.7.3	F	15.0.0	15.1.0	R5-195878
RP-85	RP-191704	1385	-	Clean-up of Annex A.7.4	F	15.0.0	15.1.0	R5-195879
RP-85	RP-191704	1386	-	Clean-up of Annex A.7.5	F	15.0.0	15.1.0	R5-195880
RP-85	RP-191704	1387	-	Clean-up of Annex A.7.6	F	15.0.0	15.1.0	R5-195881
RP-85	RP-191704	1390	-	Editorials regarding PANI header in Annex A.2.1	F	15.0.0	15.1.0	R5-195884
RP-85	RP-191704	1391	-	Generalization of C.1	F	15.0.0	15.1.0	R5-195891
RP-85	RP-191689	1392	-	Adding requirements for codec preference order and EVS configurations to C.21e	F	15.0.0	15.1.0	R5-195892
RP-85	RP-191704	1394	-	Revisiting the Scope section	F	15.0.0	15.1.0	R5-195894
RP-85	RP-191704	1395	-	Correction of IMS test case 15.30	F	15.0.0	15.1.0	R5-195957
RP-85	RP-191704	1398	-	Addition of new MO voice call scenario without preconditions when 503 service unavailable	F	15.0.0	15.1.0	R5-196011
RP-85	RP-191689	1399	-	Addition of new MO voice call scenario without preconditions when 504 server time-out	F	15.0.0	15.1.0	R5-196012
RP-85	RP-191704	1403	-	New generic procedure for MO release of IMS call	F	15.0.0	15.1.0	R5-196034
RP-85	RP-191707	1404	-	Updated of MO MTSI voice call without preconditions test case 12.12a	F	15.0.0	15.1.0	R5-196162
RP-85	RP-191707	1361	1	Clean-up of Annex A.2.16	F	15.0.0	15.1.0	R5-197032
RP-85	RP-191704	1388	1	Clean-up of Annex A.8.1	F	15.0.0	15.1.0	R5-197033
RP-85	RP-191704	1389	1	Clean-up of Annex A.8.2	F	15.0.0	15.1.0	R5-197034
RP-85	RP-191704	1393	1	Adding requirement for codec preference order to C.44	F	15.0.0	15.1.0	R5-197035
RP-85	RP-191704	1396	1	Correction of IMS session timer test cases 22.1, 22.2, 22.3, 22.5, 22.6, 22.7, 22.8	F	15.0.0	15.1.0	R5-197036

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-85	RP-191704	1397	1	Addition of new clause for generic test procedure to set up MTSI MO speech call without preconditions	F	15.0.0	15.1.0	R5-197037
RP-85	RP-191704	1400	1	Update of IMS eCall test cases 21.1 and 21.2	F	15.0.0	15.1.0	R5-197038
RP-85	RP-191704	1405	1	Addition of new test case 12.27 for codec change from AMR-WB to AMR-NB	F	15.0.0	15.1.0	R5-197039
RP-85	RP-191689	1406	1	Addition of new test case 12.27a for codec change from EVS to AMR-NB	F	15.0.0	15.1.0	R5-197040
RP-85	RP-191704	1407	1	Addition of new test case 12.28 for canceling a voice call establishment by MO UE	F	15.0.0	15.1.0	R5-197041
RP-85	RP-191689	1408	1	Addition of new test case 12.25a for MT UE not supporting EVS	F	15.0.0	15.1.0	R5-197042
RP-85	RP-191704	1409	1	Addition of new test case 18.1a for Mobile Originating Concatenated SMS	F	15.0.0	15.1.0	R5-197043
RP-85	RP-191704	1410	1	Addition of new test case 18.2a for Mobile Terminating Concatenated SMS	F	15.0.0	15.1.0	R5-197044
RP-85	RP-191704	1402	1	New IMS test case K.1.1	F	15.0.0	15.1.0	R5-197049
RP-85	RP-191704	1412	-	Title: Unify usage of dynamic payload type numbers	F	15.0.0	15.1.0	R5-197050
RP-85	RP-191704	1411	1	Adding C.21g for EPS fallback	F	15.0.0	15.1.0	R5-197224
RP-86	RP-192481	1415	-	Correction of IMS Emergency call testcase 19.4.5	F	15.1.0	15.2.0	R5-198273
RP-86	RP-192480	1418	-	Addition of a new test case for MO video cancel	F	15.1.0	15.2.0	R5-198460
RP-86	RP-192464	1420	-	New default message for 500 Server Internal Error	F	15.1.0	15.2.0	R5-198657
RP-86	RP-192480	1414	1	Correction of IMS session timer test cases 22.2, 22.5, 22.6	F	15.1.0	15.2.0	R5-198895
RP-86	RP-192481	1416	1	Addition of a new test case for emergency call via CS domain	F	15.1.0	15.2.0	R5-198896
RP-86	RP-192480	1417	1	Addition of a new test case for MO SMS failure	F	15.1.0	15.2.0	R5-198897
RP-87	RP-200071	1423	-	Corrections to SMS test case 18.1b	F	15.2.0	15.3.0	R5-200259
RP-87	RP-200071	1425	-	Corrections to Via header in PRACK, UPDATE, and BYE	F	15.2.0	15.3.0	R5-200457
RP-87	RP-200071	1426	-	Corrections to Contact header in UPDATE	F	15.2.0	15.3.0	R5-200458
RP-87	RP-200071	1427	-	Addition of SIP_305 Use Proxy message	F	15.2.0	15.3.0	R5-200864
RP-87	RP-200071	1422	1	Corrections to IMS test case 22.2	F	15.2.0	15.3.0	R5-201120
RP-87	RP-200071	1424	1	Corrections to A.1.1 and C.46 for re-registration scenarios	F	15.2.0	15.3.0	R5-201121
RP-88	RP-200593	1428	-	Adding Allow headers indicating support of UPDATE in Session Timer test cases	F	15.3.0	15.4.0	R5-201447
RP-88	RP-200593	1429	-	Fixing mix-up of UE and SS in IMS test case 22.5	F	15.3.0	15.4.0	R5-201448
RP-88	RP-200593	1430	-	Corrections to IMS Session Timer test case 22.7	F	15.3.0	15.4.0	R5-201449
RP-88	RP-200593	1431	-	Correction to the Request-URI of the ACK method	F	15.3.0	15.4.0	R5-201450
RP-88	RP-200593	1435	-	Corrections to XCAP test cases regarding rule elements	F	15.3.0	15.4.0	R5-202502
RP-88	RP-200593	1433	1	Update of speech call test case title	F	15.3.0	15.4.0	R5-202532

Meeting-1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-89	RP-201466	1437	-	Adding check to REGISTER regarding nonce-count	F	15.4.0	15.5.0	R5-203430
RP-89	RP-201466	1438	-	Correction to A.1.2 regarding WWW-Authenticate	F	15.4.0	15.5.0	R5-203432
RP-89	RP-201466	1439	-	Extending default message for NOTIFY to cover de-registration scenarios	F	15.4.0	15.5.0	R5-203433
RP-89	RP-201448	1440	-	Adding cross-references to TS 34.229-5	F	15.4.0	15.5.0	R5-203434
RP-89	RP-201448	1441	-	Removing 5G content	F	15.4.0	15.5.0	R5-203435
RP-89	RP-201466	1443	-	On checking feature tags in REGISTER	F	15.4.0	15.5.0	R5-204374
RP-89	RP-201466	1436	1	Correction to IMS TCs-wait for UE IMS de-register	F	15.4.0	15.5.0	R5-204530
RP-89	RP-201466	1442	1	Corrections of further XCAP test cases regarding rule elements	F	15.4.0	15.5.0	R5-204531

History

Document history		
V15.0.0	July 2019	Publication
V15.1.0	October 2019	Publication
V15.2.0	January 2020	Publication
V15.3.0	April 2020	Publication
V15.4.0	July 2020	Publication
V15.5.0	May 2021	Publication
V15.6.0	January 2021	Publication
V15.7.0	April 2021	Publication