ETSI TS 134 229-1 V6.3.0 (2007-10)

Technical Specification

Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Part 1: Protocol conformance specification (3GPP TS 34.229-1 version 6.3.0 Release 6)

Reference

RTS/TSGR-0534229-1v630

Keywords

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

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

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)".

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.

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.
  - For a Release 1999 UE, references to 3GPP documents are to version 3.x.y, when available.
  - For a Release 4 UE, references to 3GPP documents are to version 4.x.y, when available.
  - For a Release 5 UE, references to 3GPP documents are to version 5.x.y, when available.
  - For a Release 6 UE, references to 3GPP documents are to version 6.x.y, when available.

[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] 3GPP TS 26.234: " Transparent end-to-end Packet-switched Streaming Service (PSS); Protocols and codecs ".

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

[13] 3GPP TS 33.102: "3GPPSecurity; Security architecture".

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

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

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

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

[18] RFC 3455: "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)"

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

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

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

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

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

[24] RFC 3320: 'Signaling Compression (SigComp)'

[25] RFC 3485: 'The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)'

[26] RFC 3486: 'Compressing the Session Initiation Protocol (SIP)'

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

[28] RFC 2403: "The Use of HMAC-MD5-96 within ESP and AH".

[29] RFC 2404: "The Use of HMAC-SHA-1-96 within ESP and AH".

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

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

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

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

[34] RFC 3265: "Session Initiation Protocol (SIP) Specific Event Notification".

[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)".

[18] 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] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[42] 3GPP TS 27.060: "Packet domain; Mobile Station (MS) supporting Packet Switched services".

[43] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[44] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[45] 3GPP TS 29.207: "Policy control over Go interface".

[46] 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows".

[47] RFC 2373: "IP Version 6 Addressing Architecture".

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

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

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

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

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

[53] RFC 3556: "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[54] RFC 2833: "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

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

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

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

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
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 have 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.

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. The test case is applicable for IMS security or early IMS security.

6.2.2 Conformance requirement

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

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 and 3GPP TS 27.060 . 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 IPv6 address;

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 signaling. 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 IE.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE 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 IE. 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 IE is described in 3GPP TS 24.008.

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 B.2.2.1, 3GPP TR 33.978[59], clause 6.2.3.1.

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

Related ICS/IXIT Statement(s)

UE capable of being configured to initiate Dedicated PDP Context (Yes/No)

UE Supports IPv4 (Yes/No)

UE Supports IPv6 (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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 (early IMS security 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 (early IMS security only) step 5-9 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 "early IMS security" when applicable

Specific Message Contents:

Activate PDP Context Request (step 1)

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

*Note: 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	0001H (P-CSCF Address) (Included if "P-CSCF Server Address Request" is received)
-- Container 1 Length	16 bytes
-- Container 1 contents	IPV6 address of SS P-CSCF Server
-- container 2 Identifier	0003H (DNS Address) (Included if "DNS Server Address Request" is received)
-- Container 2 Length	16 bytes
-- Container 2 contents	IPV6 address of SS DNS Server

Case 2: UE supports only IPv4

IE	Value/Remarks
Protocol Configuration options	
- Additional Parameters	
-- container 1 Identifier	0001H (P-CSCF Address)
-- Container 1 Length	16 bytes
-- Container 1 contents	IPV4 address of SS P-CSCF encoded as per 3GPP TR 23.981[35]
-- container 2 Identifier	0003H (DNS Address) (Included if "DNS Server Address Request" is received)
-- Container 2 Length	16 bytes
-- Container 2 contents	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. The test case is applicable for IMS security or early IMS security.

6.3.2 Conformance requirement

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

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 and 3GPP TS 27.060 . 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 IPv6 address;

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 . The UE can also set the Signalling Indication attribute within the QoS IE;

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signaling. 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 IE.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE 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 IE. 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 IE is described in 3GPP TS 24.008 .

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 B.2.2.1, 3GPP TR 33.978[59], clause 6.2.3.1.

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.

Related ICS/IXIT Statement(s)

UE capable of being configured to initiate Dedicated PDP Context (Yes/No)

UE Supports IPv4 (Yes/No)

UE Supports IPv6 (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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 (early IMS security 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 (early IMS security only) step 5-9 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 'early IMS security' 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	 * 0002H (IM CN Subsystem Signaling Flag) 0 bytes

* Note: 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	0002H (IM CN Subsystem Signaling Flag)
-- Container 1 Length	0 bytes
-- container 2 Identifier	0001H (P-CSCF Address) (Included if "P-CSCF Server Address Request" is received)
-- Container 2 Length	16 bytes
-- Container 2 contents	IPV6 address of SS P-CSCF Server
-- container 3 Identifier	0003H (DNS Address) (Included if "DNS Server Address Request" is received)
-- Container 3 Length	16 bytes
-- Container 3 contents	IPV6 address of SS DNS Server

Case 2: UE supports only IPv4

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

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. The test case is applicable for IMS security or early IMS security.

7.1.2 Conformance requirement

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

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 and 3GPP TS 27.060. 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 IPv6 address;

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 signaling. 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 IE.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE 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 IE. 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 IE is described in 3GPP TS 24.008.

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

NOTE: A general-purpose PDP Context may carry both IM CN subsystem signaling and media, in case the media does not need to be authorized by Service Based Local Policy mechanisms defined in 3GPP TS 29.207 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 IE 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 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 IE 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 subclause 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, 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 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. In such a case, the use of 'IPv4 mapped addresses' as defined in RFC 2373 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.

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 B.2.2.1.

3GPP TR 23.981[35], clause 5.2.1.

3GPP TR 33.978[59], clause 6.2.3.1.

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.

Related ICS/IXIT Statement(s)

UE Supports IPv4 (Yes/No)

UE Supports "IPv6 address with embedded IPv4 address" in PCO IE (Yes/No)

UE Supports IPv4 address in PCO IE (Yes/No)

UE Supports IPv6 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via PCO (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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 (early IMS security 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 byincluding 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 (early IMS security only) step 5-9 in order to get the UE in a stable registered state

NOTE: 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: The default messages contents in annex A are used with condition 'IMS security ' or 'early IMS security' when applicable

Specific Message Contents:

Activate PDP Context Request (step 1)

Note: Containers can be in any order.

IE	**Value/Remarks**
Protocol Configuration options	
- Additional Parameters	
-- container 1 Identifier	0001H (P-CSCF Address Request);
-- Container 1 Length	0 bytes
-- container 2 Identifier	0003H (DNS Server Address Request) (Optional)
-- Container 2 Length	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	0001H (P-CSCF Address)
-- Container 1 Length	16 bytes
-- Container 1 contents	IPV6 address of SS P-CSCF Server
-- container 2 Identifier	0003H (DNS Address) (Included if "DNS Server Address Request" is received)
-- Container 2 Length	16 bytes
-- Container 2 contents	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

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. The test case is applicable for IMS security or early IMS security.

7.2.2 Conformance requirement

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

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 and 3GPP TS 27.060. 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 IPv6 address;

…

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

The methods for P-CSCF discovery are:

I.

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 , the DHCPv6 options for SIP servers RFC 3319 and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 as described in subclause 9.2.1.

II. …

The UE can freely select method I or II for P-CSCF discovery. 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 3319 . If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

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.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 and RFC 3646 or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060.

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.

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 B.2.2.1.

3GPP TR 23.981[35], clause 5.2.1.

3GPP TR 33.978[59], clause 6.2.3.1.

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.

Related ICS/IXIT Statement(s)

UE Supports IPv4 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via DHCPv4 (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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, 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 (early IMS security only) step 5-9 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 'early IMS security' 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 exeptions

Field	Value/Remarks
Options	*
- 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) **
Option code	6(Domain Server) Optionally present

*Note 1: Other options may also be present

** Note 2: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 2728[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. The test case is applicable for IMS security or early IMS security.

7.3.2 Conformance requirement

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

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 and 3GPP TS 27.060. 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 IPv6 address;

…

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

The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 , the DHCPv6 options for SIP servers RFC 3319 and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 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 IE 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 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 IE as the P-CSCF address with the highest priority.

The UE can freely select method I or II for P-CSCF discovery. 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 3319 . If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

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.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 and RFC 3646 or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060.

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.

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 B.2.2.1.

3GPP TR 23.981[35], clause 5.2.1.

3GPP TR 33.978[59], clause 6.2.3.1.

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.

Related ICS/IXIT Statement(s)

UE Supports IPv4 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via PCO (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

UE supports P-CSCF Discovery via PCO and DHCPv4(Yes/No)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 already knows DHCP server address or 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, 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 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, goe to step 5.
3	→		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.
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 (early IMS security only) step 5-9 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 'early IMS security' 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	* 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) **
Option code	6(Domain Server) Optionally present

*Note 1: Other options may also be present.

** Note 2: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 2728[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. The test case is applicable for IMS security or early IMS security.

7.4.2 Conformance requirement

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

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 and 3GPP TS 27.060. 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 IPv6 address;

…

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

The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 , the DHCPv6 options for SIP servers RFC 3319 and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 as described in subclause 9.2.1.

II. …

The UE can freely select method I or II for P-CSCF discovery. 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 3319 . If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

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.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 and RFC 3646 or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060.

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 B.2.2.1, 3GPP TR 33.978[59], clause 6.2.3.1.

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.

Related ICS/IXIT Statement(s)

UE Supports IPv6 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via DHCPv6 (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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.

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)*
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 (early IMS security only) step 5-9 in order to get the UE in a stable registered state

* Note: 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: The default messages contents in annex A are used with condition 'IMS security ' or 'early IMS security' when applicable

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

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

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

*Note: 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_ORO (6)
- option-len	2 * 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: 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: 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: 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_SIP_SERVER_D (21)
- option-len	Length of encoded domain address RFC 3319[51]
Domain-address 1	SS P-CSCF server domain Address RFC 3319[51]
option-code	OPTION_DNS_SERVERS (23)
- option-len	Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code	OPTION_DOMAIN_LIST (24)
- option-len	Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

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

*Note: 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=	NAPTR
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 2728[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. The test case is applicable for IMS security or early IMS security.

7.5.2 Conformance requirement

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

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 and 3GPP TS 27.060. 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 IPv6 address;

…

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

The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 , the DHCPv6 options for SIP servers RFC 3319 and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 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 IE 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 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 IE as the P-CSCF address with the highest priority.

The UE can freely select method I or II for P-CSCF discovery. 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 3319 . If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

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.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 and RFC 3646 or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060.

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 B.2.2.1, 3GPP TR 33.978[59], clause 6.2.3.1.

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.

Related ICS/IXIT Statement(s)

UE Supports IPv6 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via PCO (Yes/No)

UE supports P-CSCF Discovery via PCO and DHCPv6(Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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.

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)*
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 (early IMS security only) step 5-9 in order to get the UE in a stable registered state

* Note: 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: The default messages contents in annex A are used with condition 'IMS security ' or 'early IMS security' when applicable

Specific Message Contents:

Step 1: Activate PDP Context Request

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

Step 2: Activate PDP Context Accept

Options	Value/Remarks
Protocol Configuration options	(Included if "DNS Server Address Request" is received)
- Additional Parameters	
-- container 1 Identifier	0003H (DNS Address)
-- Container 1 Length	16 bytes
-- Container 1 contents	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_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: Options can be optionally present and option codes can be in any order

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

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

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

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

*Note: 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=	NAPTR
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 2728[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. The test case is applicable for IMS security or early IMS security.

7.6.2 Conformance requirement

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

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 and 3GPP TS 27.060. 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 IPv6 address;

…

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

The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 , the DHCPv6 options for SIP servers RFC 3319 and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 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 IE 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 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 IE as the P-CSCF address with the highest priority.

The UE can freely select method I or II for P-CSCF discovery. 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 3319 . If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

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.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 and RFC 3646 or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060.

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 B.2.2.1, 3GPP TR 33.978[59], clause 6.2.3.1.

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.

Related ICS/IXIT Statement(s)

UE Supports IPv6 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via DHCPv6 (Yes/No)

UE supports P-CSCF Discovery via PCO and DHCPv6 (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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.

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)*
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 (early IMS security only) step 5-9 in order to get the UE in a stable registered state

* Note: 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: The default messages contents in annex A are used with condition 'IMS security ' or 'early IMS security' 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*

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

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

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

*Note: 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=	NAPTR
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 2728[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 11, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.7 Void

7.8 Void

8 Registration

8.1 Initial registration

8.1.1 Definition and applicability

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. The test case is applicable for IMS security.

8.1.2 Conformance requirement

The ISIM application shall always be used for IMS authentication, if it is present, as described in 3GPP TS 33.203.

...

In case the UE is loaded with a UICC that does not contain the ISIM application, 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. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them in subsequent non-REGISTER requests.

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.

The initial registration procedure consists of the UE sending an unprotected initial REGISTER request and, upon being challenged, sending the integrity protected REGISTER request. The UE can register a public user identity with its contact address at any time after it has aquired 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.

The UE shall send only the initial 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, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261.

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. A public user identity may be input by the end user..

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

a) the Authorization header, with:
    - the username directive, set to the value of the private user identity;
    - the realm directive, set to the domain name of the home network;
    - the uri directive, set to the SIP URI of the domain name of the home network;
    - the nonce directive, set to an empty value; and
    - the response directive, set to an empty value.
b) the From header set to the SIP URI that contains the public user identity to be registered;
c) the To header set to the SIP URI that contains the public user identity to be registered;
d) the Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field. For the UDP the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field, while for the TCP, the response is received on the TCP connection on which the request was sent;NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, 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 protected port value see 3GPP TS 33.203.

f) the Expires header, or the expires parameter within the Contact header, set to the 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.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the 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 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;

NOTE: IMS Rel-5 requires the UE to support integrity protection while Rel-6 requires the UE to support both integrity and confidentiality protection.

i) the Supported header containing the option tag "path"; and

j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4).

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in 3GPP TS 24.229 subclause 5.1.1.5.1.

Authentication is achieved via the registration, re-registration and deregistration procedures . 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 as described in RFC 3329. If the header 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 based on the static list and parameters it received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header 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 as the shared key. The UE shall use the parameters received in the Security-Server header 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 using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the realm directive set to the value as received in the realm directive in the WWW Authenticate header, the private user identity and the authentication challenge response calculated by the UE using RES and other parameters, as described in RFC 3310. The UE shall also insert the Security-Client header that is identical to the Security-Client header 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 into the request, by mirroring in it the content of the Security-Server header 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 integrity protected REGISTER request, 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

- use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

NOTE: In this case, the UE will send requests towards the P-CSCF over the newly established set of security associations. Responses towards the P-CSCF that are sent via UDP will be sent over the newly established set of security associations. 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, 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.

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 value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

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

e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and

f) 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.

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 users registrar (S-CSCF) as described in RFC 3680.

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.

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 set to a SIP URI that contains the public user identity used for subscription;

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

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

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

f) a P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4); and

g) a Contact header set to contain the same IP address or FQDN, and with the protected server port value as in the initial registration.

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

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and
- include the protected server port in any Contact header that is otherwise included.

….

The UE shall insert a P-Access-Network-Info header 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. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

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 of the received response.

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 "terminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered.

NOTE: 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. 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.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.1A, 5.1.1.2, 5.1.1.3, 5.1.1.5.1, 5.1.2.1 and 5.1.2A.1.

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, according to the procedures described in 3GPP TS 23.003 [32] clause 13 or alternatively uses the values retrieved from ISIM; 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

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, 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].

Related ICS/IXIT Statement(s)

- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)

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 set up a temporary set of security associations and send another REGISTER request, over those security associations.

4) 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. 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 request over the newly established security associations.

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.

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_IpSecAlgorithm PIXIT.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
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 temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 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 A1 "Initial unprotected REGISTER"

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 with condition A2 "Subsequent REGISTER sent over security associations

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

200 OK for SUBSCRIBE (Step 6)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5

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

8.1.5 Test requirements

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. The test case is applicable for IMS security.

8.2.2 Conformance requirement

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the 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.

The UE shall protect the REGISTER request using a security association, 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.

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

a) an Authorization header, with:

- the username directive set to the value of the private user identity;
- the realm directive, set to the value as received in the realm directive in the WWW Authenticate header;
- the uri directive, set to the SIP URI of the domain name of the home network;
- the nonce directive, set to last received nonce value; and
- the response directive, set to the last calculated response;

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

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

d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and for the UDP the protected server port value bound to the security association, while for the TCP, the response is received on the TCP connection on which the request was sent;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, 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.

f) an Expires header, or an expires parameter within the Contact header, set to 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.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) a Security-Client header field, set to specify the security mechanism 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;

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

j) the Supported header containing the option tag "path"; and

k) the P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4).

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

a) store the new expiration time of the registration for this public user identity found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

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

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1. On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

NOTE: 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. 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.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.4.

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].

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

UE supports IPSec ESP confidentiality protection (Yes/No)

Test procedure

1-8) The same procedure as in subclause 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 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 8.1.4)	The same messages as in subclause 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 A2 "Subsequent REGISTER sent over security associations" 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
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

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 condition A2 "Subsequent REGISTER sent over security associations" 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, may or may not be the same as in step 1
spi-s	new SPI number of the inbound SA at the protected server port, may or may not be the same as in step 1
port-c	new protected client port needed for the setup of new pairs of security associations, may or may not be the same as in step 1
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 condition A2 "Subsequent REGISTER sent over security associations" 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, may or may not be the same as in step 1 and 3
spi-s	new SPI number of the inbound SA at the protected server port, may or may not be the same as in step 1 and 3
port-c	new protected client port needed for the setup of new pairs of security associations, may or may not be the same as in step 1 or 3
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 and applicability

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. The test case is applicable for IMS security.

8.3.2 Conformance requirement

The UE can deregister a previously registered 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, 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.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities.

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

a) an Authorization header, with;

   - the username directive, set to the value of the private user identity;
   - the realm directive, set to the value as received in the realm directive in the WWW Authenticate header;
   - the uri directive, set to the SIP URI of the domain name of the home network;

- the nonce directive, set to last received nonce value; and
- the response directive, set to the last calculated response value;

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

c) a To header set to the SIP URI that contains the public user identity to be deregistered;

d) a Contact header set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and the protected server port value bound to the security association;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, 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.

f) a Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) a Security-Client header field, set to specify the security mechanism 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 [19] and RFC 3329 [48];

i) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication; and

j) a P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4).

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.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and the security association 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 containing a value of zero).

NOTE: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered), the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.6.

8.3.3 Test purpose

1) To verify that the UE sends a correctly composed initial REGISTER request with an Expires header or expires parameter set to 0 to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.1.6.

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].

Related ICS/IXIT Statement(s)

Method of triggering the UE to deregister from IMS services Yes/No

IMS security (Yes/No)

Test procedure

1) The UE is triggered by MMI to initiate a deregistration procedure

2) 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

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends deregistration for IMS services. (Register request with Expires header set to 0).
2	←		200 OK	The SS responds REGISTER with 200 OK

Specific message contents

REGISTER (step 1)

SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.6 the UE sends an initial REGISTER request where the Request-URI and the headers have been correctly populated according to the REGISTER common message definition in annex A.1.1condition A2 without the 'Supported' header and with the following exception:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and protected server port of UE or *
expires	*0* (if present, see Rule)
Expires	**(if present, see Rule)**
delta-seconds	*0*

Rule: if the addr-spec parameter of **Contact** header is *, expires parameter must not be present and **Expires** header is mandatory, if the addr-spec parameter of **Contact** header is not *, expires parameter is mandatory and **Expires** header must not be present.

8.3.5 Test Requirements

SS shall check in step 1 that the de-register request sent by the UE have the headers correctly populated as per the default message 'REGISTER' in annex A.1.1condition A2, except for the headers described in 8.3.4.

8.4 Invalid behaviour- 423 Interval too brief

8.4.1 Definition and applicability

Test to verify that the UE another REGISTER request using a correct expiration timer when a registration attempt was rejected with a 423 (Interval Too Brief) response. The test case is applicable for IMS security.

8.4.2 Conformance requirement

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.2.

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.

Related ICS/IXIT Statement(s)

<To be added>

IMS security (Yes/No)

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 because the expiration time of the resource refreshed by the request is too short.

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.

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.2steps 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.

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 Initial registration for early IMS security

8.5.1 Definition and applicability

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains either SIM application, 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. The test case is applicable for UE supporting early IMS security only.

8.5.2 Conformance requirement

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include header fields or header field values as required by RFC3329. The From header, To header, Contact header, Expires header, Request URI and Supported header shall be set according clause 5.1.1.2 of TS 24.229.

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according clause 5.1.1.2 of TS 24.229.

The UE shall support SIP compression as described in TS 24.229 subclause 8.1.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the UE creates the compartment is implementation specific.

The UE shall use the temporary public user identity (IMSI-derived IMPU, cf. section 6.1.2) only in registration messages (i.e. initial registration, re-registration or de-registration), but not in any other type of SIP requests.

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.

…

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in TS 23.003. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

…

When early IMS security is used for registering an UE, the IMSI-derived IMPU shall be used for all registration procedures initiated by the UE (i.e., initial registration, re-registration and mobile-initiated de-registration).

…

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 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.

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 set to a SIP URI that contains the public user identity used for subscription;

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

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

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

f) a P-Access-Network-Info header set as specified for the access network technology; and

g) a Contact header set to contain the same IP address or FQDN, and with the protected server port value as in the initial registration.

Reference(s)

3GPP TR 33.978[58], clauses 6.2.3.1, 6.2.4, 3GPP TS 24.229[10], clause 5.1.1.3.

8.5.3 Test purpose

1) To verify that UE correctly derives a temporary public user identity from the IMSI parameter according to the procedures described in 3GPP TS 23.003 [32] clause 13; and

2) To verify that UE correctly derives a home network domain name from the IMSI parameter according to the procedures described in 3GPP TS 23.003 [32] clause 13 or alternatively uses the values retrieved from ISIM; and

3) To verify that the UE sends a correctly composed initial REGISTER request to S-CSCF via the discovered P-CSCF, according to 3GPP TS 33.978 [58] clause 6.2.3.1; and

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

5) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER, 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

6) 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

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

8.5.4 Method of test

Initial conditions

UE contains either SIM application, 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. SS is able to perform security mechanism according to 3GPP TS 33.978 [58] clause 6.2.3.4.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1) The UE initiates IMS registration indicating support of early IMS security. SS waits for the UE to send an initial REGISTER request.

2) The SS responds to the REGISTER request with valid 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 valid 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 early IMS security 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 early IMS security"

200 OK for REGISTER (Step 2)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A2 'early IMS security'

SUBSCRIBE (Step 3)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4 with condition A2 'early IMS security'.

200 OK for SUBSCRIBE (Step 4)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5 with condition A2 'early IMS security'

NOTIFY (Step 5)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with condition A2 'early IMS security'

200 OK for NOTIFY (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

8.5.5 Test requirements

Step 1: SS shall check that in accordance to the 3GPP TR 33.978 [58] clause 6.2.3.1 the UE sends a REGISTER request as follows:

a) the Authorization header is not present;

Step 3: 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.

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 unprotected port in the initial REGISTER.

8.6 Initial registration for combined IMS security and early IMS security against a network with early IMS support only

8.6.1 Definition and applicability

Test to verify that the UE can correctly register to IMS services in a network with support for early IMS security 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. The test case is applicable when both IMS security and early IMS security are supported.

8.6.2 Conformance requirement

The ISIM application shall always be used for IMS authentication, if it is present, as described in 3GPP TS 33.203.

…

In case the UE is loaded with a UICC that does not contain the ISIM application, 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

…

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 application on a UICC, the ISIM application is used for IMS authentication, as described in 3GPP TS 33.203.

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, mobile-initiated deregistration. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them in subsequent non-REGISTER requests.

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.

…

The initial registration procedure consists of the UE sending an unprotected initial REGISTER request and, upon being challenged, sending the integrity protected REGISTER request. The UE can register a public user identity with its contact address at any time after it has aquired 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.

The UE shall send only the initial 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, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261.

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. A public user identity may be input by the end user.

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

a) an Authorization header, with:

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

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

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

d) a Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field. For the UDP the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field, while for the TCP, the response is received on the TCP connection on which the request was sent;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, 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.

f) an Expires header, or the expires parameter within the Contact header, set to the 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.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the 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 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;

i) the Supported header containing the option tag "path"; and

j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology.

…

3. ME supports both, IMS network supports early IMS security only.

   The ME shall check the smartcard application in use.

If a SIM is in use, then it shall start with an Early IMS security procedure, else it shall start with the fully compliant IMS Registration procedure.

In the second case, the early IMS 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 an early IMS 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 early IMS security.

...

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include header fields or header field values as required by RFC3329. The From header, To header, Contact header, Expires header, Request URI and Supported header shall be set according clause 5.1.1.2 of TS 24.229.

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according clause 5.1.1.2 of TS 24.229.

The UE shall support SIP compression as described in TS 24.229 subclause 8.1.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the UE creates the compartment is implementation specific.

The UE shall use the temporary public user identity (IMSI-derived IMPU, cf. section 6.1.2) only in registration messages (i.e. initial registration, re-registration or de-registration), but not in any other type of SIP requests.

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.

…

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in TS 23.003. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

…

When early IMS security is used for registering an UE, the IMSI-derived IMPU shall be used for all registration procedures initiated by the UE (i.e., initial registration, re-registration and mobile-initiated de-registration).

…

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 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.

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 set to a SIP URI that contains the public user identity used for subscription;

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

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

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

f) a P-Access-Network-Info header set as specified for the access network technology; and

g) a Contact header set to contain the same IP address or FQDN, and with the protected server port value as in the initial registration.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.1A, C.2, 5.1.1.1A, 5.1.1.2

3GPP TR 33.978[58], clauses 6.2.6, 6.3.3.1, 6.2.4

3GPP TS 24.229[10], clause 5.1.1.3

8.6.3 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, according to the procedures described in 3GPP TS 23.003 [32] clause 13 or alternatively uses the values retrieved from ISIM; and

2) To verify that UE correctly derives a home network domain name from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003 [32] clause 13 or alternatively uses the values retrieved from ISIM; and

3) To verify that after receiving a 420 (Bad Extension) response from S-CSCF for the initial REGISTER sent, the UE sends a correctly composed initial REGISTER request to S-CSCF via the discovered P-CSCF, according to 3GPP TS 33.978 [58] clause 6.2.3.1; and

4) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER, 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 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

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

8.6.4 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, 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. SS is able to perform security mechanism according to 3GPP TS 33.978 [58] clause 6.2.3.4.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Early IMS security (Yes/No)

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 early IMS security. 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 valid 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 early IMS security 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"

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 early IMS security"

200 OK for REGISTER (Step 4)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A2 'early IMS security'

SUBSCRIBE (Step 5)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4 with condition A2 'early IMS security'.

200 OK for SUBSCRIBE (Step 6)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5 with condition A2 'early IMS security'

NOTIFY (Step 7)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with condition A2 'early IMS security'

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

8.6.5 Test requirements

Step 1: SS shall check that in accordance to the 3GPP TS 24.229[10] clause 5.1.1.2 the UE sends a REGISTER request as follows:

a) the Authorization header is present;

Step 3: SS shall check that in accordance to the 3GPP TR 33.978 [58] clause 6.2.3.1 the UE sends a REGISTER request as follows:

a) the Authorization header is not present;

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.

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 unprotected port in the initial REGISTER.

8.7 Initial registration for combined IMS security and early IMS security with SIM application

8.7.1 Definition and applicability

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains a SIM 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. The test case is applicable when both IMS security and early IMS security are supported.

8.7.2 Conformance requirement

4. ME and IMS network support both.

   The ME shall check the smartcard application in use.

   If a USIM/ISIM application is in use, then the ME shall start with the fully compliant IMS security registration procedure. The network, with receiving the initial REGISTER request, receives indication that the IMS UE is fully compliant and shall continue as specified by TS 33.203 [2].

   If a SIM is in use, then the ME shall start with the Early IMS security registration procedure. If the ME starts with the fully compliant IMS security registration procedure when a SIM is in use, this is an error case to be handled as follows: when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that a SIM is in use and returns an error. The S-CSCF shall answer with a 403 (Forbidden). After receiving the 403 response, the UE shall stop the attempt to register with this network.

…

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include header fields or header field values as required by RFC3329. The From header, To header, Contact header, Expires header, Request URI and Supported header shall be set according clause 5.1.1.2 of TS 24.229.

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according clause 5.1.1.2 of TS 24.229.

The UE shall support SIP compression as described in TS 24.229 subclause 8.1.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the UE creates the compartment is implementation specific.

The UE shall use the temporary public user identity (IMSI-derived IMPU, cf. section 6.1.2) only in registration messages (i.e. initial registration, re-registration or de-registration), but not in any other type of SIP requests.

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.

…

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in TS 23.003. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

…

When early IMS security is used for registering an UE, the IMSI-derived IMPU shall be used for all registration procedures initiated by the UE (i.e., initial registration, re-registration and mobile-initiated de-registration).

…

.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 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.

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 set to a SIP URI that contains the public user identity used for subscription;

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

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

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

f) a P-Access-Network-Info header set as specified for the access network technology; and

g) a Contact header set to contain the same IP address or FQDN, and with the protected server port value as in the initial registration.

Reference(s)

3GPP TR 33.978[58], clauses 6.2.6, 6.2.3.1, 6.2.4, 3GPP TS 24.229[10], clause 5.1.1.3.

8.7.3 Test purpose

1) To verify that the UE initiate the early IMS security registration procedure when a SIM application is in use, even if the UE has support for IMS security; and

2) To verify that UE correctly derives a temporary public user identity from the IMSI parameter in the SIM according to the procedures described in 3GPP TS 23.003 [32] clause 13; and

3) To verify that UE correctly derives a home network domain name from the IMSI parameter in the SIM, according to the procedures described in 3GPP TS 23.003 [32] clause 13; and

4) To verify that the UE sends a correctly composed initial REGISTER request to S-CSCF via the discovered P-CSCF, according to 3GPP TS 33.978 [58] clause 6.2.3.1; and

5) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER, 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

6) 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

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

8.7.4 Method of test

Initial conditions

UE contains a SIM application only 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. SS is able to perform security mechanism according to 3GPP TS 33.978 [58] clause 6.2.3.4.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1) The UE initiates IMS registration indicating support of early IMS security. SS waits for the UE to send an initial REGISTER request.

2) The SS responds to the REGISTER request with valid 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 valid 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 early IMS security 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 early IMS security"

200 OK for REGISTER (Step 2)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A2 'early IMS security'

SUBSCRIBE (Step 3)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4 with condition A2 'early IMS security'.

200 OK for SUBSCRIBE (Step 4)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5 with condition A2 'early IMS security'

NOTIFY (Step 5)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with condition A2 'early IMS security'

200 OK for NOTIFY (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

8.7.5 Test requirements

Step 1: SS shall check that in accordance to the 3GPP TR 33.978 [58] clause 6.2.3.1 the UE sends a REGISTER request as follows:

a) the Authorization header is not present;

Step 3: 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.

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 unprotected port in the initial REGISTER.

8.8 User initiated re-registration for early IMS

8.8.1 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 early IMS security.

8.8.2 Conformance requirement

The UE can perform the reregistration of a previously registered public user identity with its contact address at any time after the initial registration has been completed. The UE shall perform the reregistration over the existing set of security associations that is associated with the related 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 over the existing set of security associations 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.

…

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

a) store the new expiration time of the registration for this public user identity found in the To header value;

…

Unlike in full IMS security, the private user identity is not included in the REGISTER requests when early IMS security is used for registration, re-registration and mobile-initiated de-registration procedures. Subsequently, all REGISTER requests from the UE shall use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. Otherwise, the I-CSCF would be unable to derive the private user identity that is needed to query the HSS in certain Cx messages.

…

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include header fields or header field values as required by RFC3329. The From header, To header, Contact header, Expires header, Request URI and Supported header shall be set according clause 5.1.1.2 of TS 24.229.

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according clause 5.1.1.2 of TS 24.229.

The UE shall support SIP compression as described in TS 24.229 subclause 8.1.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the UE creates the compartment is implementation specific.

The UE shall use the temporary public user identity (IMSI-derived IMPU, cf. section 6.1.2) only in registration messages (i.e. initial registration, re-registration or de-registration), but not in any other type of SIP requests.

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.

…

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in TS 23.003. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

…

When early IMS security is used for registering an UE, the IMSI-derived IMPU shall be used for all registration procedures initiated by the UE (i.e., initial registration, re-registration and mobile-initiated de-registration).

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.4, 3GPP TR 33.978[58], clauses 6.1.2, 6.2.3.1, 6.2.4

8.8.3 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) Upon receiving 200 OK for REGISTER, the UE shall store the new expiration time of the registration for this public user identity.

8.8.4 Method of test

Initial conditions

UE contains either SIM application, 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. SS is able to perform security mechanism according to 3GPP TS 33.978 [58] clause 6.2.3.4.

Related ICS/IXIT Statement(s)IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1-6) The same procedure as in subclause 8.5.4 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, Authorization, Expires, Security-Client, Security-verify, 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 8.5.4)	The same messages as in subclause 8.5.4 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 8.5.4 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 early IMS security'.

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 early IMS security'.

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 early IMS security'.

200 OK for REGISTER (Step 12)

Use the default message '200 OK for REGISTER' in annex A.1.3.

8.8.5 Test requirements

1. The UE shall in step 7 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 9 send the REGISTER request within 600 seconds from the time instant that it receives 200 OK from the SS in step 8.

3. The UE shall in step 11 send the REGISTER request within 1200 seconds from the time instant that it receives 200 OK from the SS in step 10.

8.9 Mobile initiated de-registration for early IMS

8.9.1 Definition and applicability

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. The test case is applicable for early IMS security.

8.9.2 Conformance requirement

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

…

Unlike in full IMS security, the private user identity is not included in the REGISTER requests when early IMS security is used for registration, re-registration and mobile-initiated de-registration procedures. Subsequently, all REGISTER requests from the UE shall use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. Otherwise, the I-CSCF would be unable to derive the private user identity that is needed to query the HSS in certain Cx messages.

…

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include header fields or header field values as required by RFC3329. The From header, To header, Contact header, Expires header, Request URI and Supported header shall be set according clause 5.1.1.2 of TS 24.229.

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according clause 5.1.1.2 of TS 24.229.

The UE shall support SIP compression as described in TS 24.229 subclause 8.1.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the UE creates the compartment is implementation specific.

The UE shall use the temporary public user identity (IMSI-derived IMPU, cf. section 6.1.2) only in registration messages (i.e. initial registration, re-registration or de-registration), but not in any other type of SIP requests.

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.

…

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in TS 23.003. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

…

When early IMS security is used for registering an UE, the IMSI-derived IMPU shall be used for all registration procedures initiated by the UE (i.e., initial registration, re-registration and mobile-initiated de-registration).

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.6, 3GPP TR 33.978[58], clauses 6.1.2, 6.2.3.1, 6.2.4

8.9.3 Test purpose

1) To verify that the UE sends a correctly composed initial REGISTER request with an Expires header or expires parameter set to 0 to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.1.6.

8.9.4 Method of test

Initial conditions

UE contains either SIM application, ISIM and USIM applications or only USIM application on UICC. UE is 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 the last step.

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. SS is able to perform security mechanism according to 3GPP TS 33.978 [58] clause 6.2.3.4.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Early IMS security (Yes/No

Test procedure

1) The UE is triggered by MMI to initiate a deregistration procedure
2) 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

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends deregistration for IMS services. (Register request with Expires header set to 0).
2	←		200 OK	The SS responds REGISTER with 200 OK

Specific message contents

REGISTER (step 1)

SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.6 the UE sends an initial REGISTER request according to the REGISTER common message definition in annex A.1.1condition A3 without the 'Supported' header and with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and unprotected server port of UE or *
expires	*0* (if present, see Rule)
Expires	(if present, see Rule)
delta-seconds	*0*

Rule: If the addr-spec parameter of **Contact** header is *, expires parameter must not be present and **Expires** header is mandatory, if the addr-spec parameter of **Contact** header is not *, expires parameter is mandatory and **Expires** header must not be present.

8.9.5 Test Requirements

SS shall check in step 1 that the de-register request sent by the UE have the headers correctly populated as per the default message 'REGISTER' in annex A.1.1condition A3, except for the headers described in 8.9.4.

9 Authentication

9.1 Invalid Behaviour – MAC Parameter Invalid

9.1.1 Definition

To test that the UE when receiving an invalid 401 (Unauthorized) response to its initial REGISTER request behaves correctly. This procedure is described in 3GPP TS 24.229 [10] clause 5.1.1.5. The test case is applicable for IMS security.

9.1.2 Conformance requirement

When the network requires 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

…

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 directive and an empty response directive, 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 directive (see 3GPP TS 33.102).

NOTE: In the case of the SQN being out of range, a response directive can be included by the UE, based on the procedures described in RFC 3310. 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);

- populate 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

- not create a temporary set of security associations.

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.5.

9.1.3 Test purpose

1) To verify that after receiving a 401 (Unauthorized) response from S-CSCF for the initial REGISTER sent, the UE checks the validity of the received authentication challenge, as described in 3GPP TS 33.203 [14] i.e. the locally calculated XMAC must match 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) received by the UE does not match the value of locally calculated XMAC:

- the UE responds with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid and:
- this subsequent REGISTER request contains no AUTS directive and an empty response directive, i.e. no authentication challenge response- 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.

9.1.4 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 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.

Related ICS/IXIT Statement(s)

<To be added>

IMS security (Yes/No)

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 in 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 and the CK and IK values are not included
    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 b)
5) SS waits for the UE to send a second Registration message indicating that the received 401 (Unauthorized) message was invalid

Note: From this point onward the SS shall ignore any Registration message sent by the UE.

6) SS sends a 403 (Forbidden) message to the UE (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
				Note: From this point onward the SS shall ignore any Registration message sent by the UE.
6	←		403 Forbidden	The SS sends this message to get the UE in a stable state.

Specific message contents

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 (Step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A1

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
Security-Verify	Header must not appear in the request
Authorization	
response	It should be present but empty
auth-param	If present it should not contain the auts='<base 64 encoded value>' directive
nonce-count	value or presence of the parameter not to be checked

403 FORBIDDEN (Step 6)

Use the default message '403 FORBIDDEN' in annex A.3.2.

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 an invalid 401 (Unauthorized) response to its initial REGISTER request behaves correctly. This procedure is described in 3GPP TS 24.229 [10] clause 5.1.1.5. The test case is applicable for IMS security.

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

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 as described in RFC 3329. If the header 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 based on the static list and parameters it received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header 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 as the shared key. The UE shall use the parameters received in the Security-Server header 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 using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response calculated by the UE using RES and other parameters, as described in RFC 3310. The UE shall also insert the Security-Client header that is identical to the Security-Client header 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 into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the integrity 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.

…

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 directive and an empty response directive, 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 directive (see 3GPP TS 33.102).

NOTE: In the case of the SQN being out of range, a response directive can be included by the UE, based on the procedures described in RFC 3310.

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);

- populate 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

- not create a temporary set of security associations.

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.5.

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 reacts correctly:

3) To verify after a failed authentication attempt if the UE on 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 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]. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Related ICS/IXIT Statement(s)

<To be added>

IMS security (Yes/No)

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 in 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 and the CK and IK values are not included

    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 5, 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 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.

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 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 must exist, but value not to be checked
auth-param	auts= LDQUOT auts-value RDQUOT, auts-value not to be checked
nonce-count	value or presence of the parameter not to be checked

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 directive; 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;
- 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 and applicability

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. The test case is applicable for IMS security or early IMS security.

10.1.2 Conformance requirement

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.

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 5.1.2.2, 3GPP TR 33.978[59], clause 6.2.3.1.

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 SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

<To be added>

IMS security (Yes/No)

Early IMS security (Yes/No)

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 (early IMS security 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 'early IMS security' 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 and applicability

Test to verify that the UE can correctly process the network initiated deregistration request. The test case is applicable for IMS security or early IMS security.

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 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").

NOTE 3: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY containing the deregistration event) will not reach the UE.

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 (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Early IMS security (Yes/No)

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 'early IMS security' 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?>* *<reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='1' state='full'>* *<registration aor=*'px_PublicUserIdentity' *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=*'px_AssociatedTelUri' *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>*

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 and applicability

Test to verify that the UE can correctly process the network initiated re-authentication request and re-authenticate the user before the registration expires, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.2. The test case is applicable for IMS security.

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 expiry attribute within 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 identitity, 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 5.1.1.5.2.

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 (as controlled by px_RegisterExpiration) 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].

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

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) Continue test execution with the Generic test procedure in Annex C.2, step 7.

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	←→		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

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

Message-body	*<?xml version='1.0?>*
	<reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='1' state='partial'>
	  <registration aor='px_PublicUserIdentity' *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>

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 MO Call Successful with preconditions (Rel-5)

12.1.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated call setup and release when using preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1. The test case is applicable for IMS security or early IMS security.

12.1.2 Conformance requirement

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and
- include the protected server port in any Contact header that is otherwise included.

….

The UE shall insert a P-Access-Network-Info header 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. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4 of TS 24.229).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

Upon generating an initial INVITE request, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;
- indicate the requirement of precondition and specify it using the Require header mechanism.

….

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session.

Usage of SDP by the UE:

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.
2. An INVITE request generated by a UE shall contain SDP payload. The SDP payload shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP payload with the most preferred codec listed first. In addition, the calling user shall indicate the desired QoS for the session, using the segmented status type. In an initial INVITE request the UE shall indicate that it mandates local QoS and that this precondition is not yet satisfied, i.e. or the local segment the UE shall include the following preconditions:

   a) a desired-status attribute line set in accordance with RFC 3312 [30] in the following manner:

      - the precondition-type attribute set to "qos";
      - the strength attribute attribute set to "mandatory";
      - the status-type attribute set to "local"; and
      - the direction-tag attribute in accordance with the direction of the related media stream; and

   b) a current-status attribute line set in accordance with RFC 3312 [30] in the following manner:

      - the precondition-type attribute set to "qos";
      - the status-type attribute set to "local"; and
      - the direction-tag attribute set to "none".

3. Providing that the INVITE request received by the UE contains an SDP offer including one or more "m=" media descriptions, the first 183 (Session Progress) provisional response that the UE sends, shall contain the answer for the SDP received in the INVITE. The said SDP answer shall reflect the called user's terminal capabilities and user preferences.
4. When the UE sends a 183 (Session Progress) response with SDP payload including one or more "m=" media descriptions, it shall request confirmation for the result of the resource reservation at the originating end point.
5. During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description.
6. 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, 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 [56] to specify the required bandwidth allocation for RTCP.

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 [13].

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifer will typically get the value of zero.

7. 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 2833 [23].
8. 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 [54] and perform the action outlined in subclause 9.2.5.
9. If a PDP context is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 [26] and RFC 3311 [29].
10. If the UE builds SDP 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 2: The UE may be attempting a session establishment through multiple networks with different policies and potentially may 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.

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], clauses 5.1.2A.1, 5.1.3 and 6.1, 3GPP TR 33.978[59], clause 6.2.3.1.

12.1.3 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.

12.1.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with a 183 Session in Progress response

NOTE: SS is not expected to take care of the media, so the IP address and port could be assigned so that the SS is listening to it, but may discard the RTP packets received.

4) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

5) SS responds to the PRACK request with valid 200 OK response.

6) 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 request of step 1 or step 4 already contained the final offer with preconditions met.

7) SS responds to the UPDATE request (if UE sent one) with valid 200 OK response.

8) SS responds to the INVITE request with 180 Ringing response.

9) SS waits for the UE to send a PRACK request.

10) SS responds to the PRACK request with valid 200 OK response.

11. SS responds to the INVITE request with valid 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 valid 200 OK response.

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
2	←		100 Trying	The SS responds with a 100 Trying provisional response
3	←		183 Session in Progress	The SS responds with an SDP answer indicating the medias and codecs acceptable for SS
4	→		PRACK	UE acknowledges the receipt of 183 response with PRACK and optionally offers second SDP that indicates one agreed codec per media and possibly indicates preconditions as met after having reserved the resources with GPRS
5	←		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.
6	→		UPDATE	Optional step: UE sends an UPDATE after having reserved the resources with GPRS procedures for PDP context used for the media
7	←		200 OK	Optional step : The SS responds UPDATE with 200 OK and indicates having reserved the resourced for the virtual remote UE
8	←		180 Ringing	The SS responds INVITE with 180 Ringing to indicate that the virtual remote UE has started ringing.
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

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 MO call setup' in annex A.2.1 with the exception that Require header shall contain the "precondition" tag.

For the contents of the SDP body see test requirement details.

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
Require	
option-tag	*precondition*
Message-body	SDP body of the 183 response copied from the received INVITE but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - optional "a=sendonly" line inverted to "a=recvonly" and vice versa - the "a=" lines describing the current and desired state of the preconditions, updated as follows: a=curr:qos local [direction-tag] (* a=curr:qos remote none a=des:qos mandatory local [direction-tag] (* a=des:qos mandatory remote [direction-tag] (* a=conf:qos remote [direction-tag] (** *) The value of direction-tags in 183 must be the inverse from those of INVITE (both a= lines for local and remote). If the INVITE contained the direction-tag as "recv" the 183 must have it as "send" and vice versa. The value "none" or "sendrecv" will be kept as is. The value for direction tag of des:qos remote must be the same as for local. The value for direction tag of curr:qos local and remote must be the inverse of direction tag of curr:qos local within the INVITE. **) The value of direction-tag for conf:qos remote shall be the same as for des: qos mandatory remote.

PRACK (Step 4)

Use the default message 'PRACK' in annex A.2.4 with the exception that Require header shall contain the "precondition" tag.

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 must be modified as follows for the 200 OK response: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - optional "a=sendonly" line inverted to "a=recvonly" and vice versa; 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 [direction-tag] (1 a=curr:qos remote [direction-tag] (2 a=des:qos mandatory local [direction-tag] (3 a=des:qos mandatory remote [direction-tag] (3 a=conf:qos remote [direction-tag] (4 1) The value of direction-tag in a=curr qos local line of 200 must be the inverse of that in the a=curr:qos local line of PRACK. If the PRACK contained the direction-tag as "recv" the 200 must have it as "send" and vice versa. The values "none" and "sendrecv" will be kept as is. 2) The value of direction-tag in a=curr qos remote line of 200 must be the inverse from the a=curr:qos local line of PRACK. 3) The value of direction-tags in a=des lines of 200 must be the inverse from those of PRACK (both a= lines for local and remote). If the PRACK contained the direction-tag as "recv" the 200 must have it as "send" and vice versa. The value "sendrecv" will be kept as is. 4) The value of direction-tag for the optional line conf:qos remote shall be the same as for des: qos mandatory remote. This line is only included if a=curr:qos remote is still "none".

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 exception that Require header shall contain the "precondition" tag.

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 as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - optional "a=sendonly" line inverted to "a=recvonly" and vice versa; 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 [direction-tag] (1 a=curr:qos remote [direction-tag] (2 a=des:qos mandatory local [direction-tag] (3 a=des:qos mandatory remote [direction-tag] (3 1) The value of direction-tag in a=curr qos local line of 200 must be the inverse of that in the a=curr:qos local line of UPDATE. If the UPDATE contained the direction-tag as "recv" the 200 must have it as "send" and vice versa. The value "sendrecv" will be kept as is. 2) The value of direction-tag in a=curr qos remote line of 200 must be the inverse from the a=curr:qos local line of UPDATE. 3) The value of direction-tags in a=des lines of 200 must be the inverse from those of UPDATE (both a= lines for local and remote). If the UPDATE contained the direction-tag as "recv" the 200 must have it as "send" and vice versa. The value "sendrecv" will be kept as is.

180 Ringing for INVITE (Step 8)

Use the default message '180 Ringing for INVITE' in annex A.2.6.

PRACK (Step 9)

Use the default message 'PRACK' in annex A.2.4 with the following exception:

Header/param	**Value/remark**
Cseq	
value	- if Steps 6-7 did not take place: value as in PRACK from Step 4 incremented by one. - If Steps 6-7 took place: value as in UPDATE from Step 6 incremented by one.

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 with the following exceptions:

Header/param	Value/remark
Record-Route	
rec-route	Same value as in the 180 response
Contact	
addr-spec	Same value as in the 180 response

ACK (Step 12)

Use the default message 'ACK' in annex A.2.7.

BYE (Step 13)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 14)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

12.1.5 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 1: the UE shall send an INVITE message with correct content. The UE shall include the following lines in the SDP body:

- All mandatory SDP lines, as specified in SDP grammar in RFC 4566 [27] appendix A, including:
    - "o=" line indicating e.g. the session identifier and the IP address of the UE;
    - "c=" line indicating the IP address of the UE for receiving the media flow;
- Media description lines for the media proposed by UE for the MO call. For each type of offered media the following lines must exist within the SDP:
    - "m=" line describing the media type, transport port and protocol used for media and media format;
    - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media , however this line may be missing if the media type is something else than "video" or "audio" or the SDP contains "a=sendonly" line, according to RFC 3264 [30];
    - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line:
    - either a=sendonly, a=recvonly or a=sendrecv line. The directionality indicated by this line must be the same as indicated by the a=curr:qos local line for preconditions
    - four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]. At this stage of the call setup the lines shall be as follows:
a=curr:qos local [none, send, recv or sendrecv]
a=curr:qos remote none
a=des:qos mandatory local [send, recv or sendrecv]
a=des:qos [none, optional or mandatory] remote [send, recv or sendrecv]
The direction tag for remote shall be the same as for local. These four "a=" lines may appear in any order.

...

Step 4: the UE shall send a PRACK request with the correct content. The UE may include a SDP body in the PRACK request In that case the following lines shall be included in the SDP body of PRACK:

- All mandatory SDP lines are present; and
- "o" line shall be the same like in INVITE request, except that the version number shall be incremented by one; and
- SDP must contain at least as many media description lines as the SDP in the INVITE contained; and
- The "a=" lines for preconditions in the PRACK shall be like for INVITE in step 1 but with the following exceptions:
    - in attribute line a=curr:qos local the direction-tag may have either the value "none" or the same value that the direction-tag has in the attribute line a=des:qos mandatory local. The latter case indicates that the UE has already met its local preconditions.
    - in attribute line a=des:qos [strength-tag] remote [direction-tag] the strength-tag must be "mandatory" (according to what SS answered in 183 response)
- either a=sendonly, a=recvonly or a=sendrecv line. The directionality indicated by this line must be the same as indicated by the a=curr:qos local line for preconditions

...

Step 6: the UE may conditionally send an UPDATE request with the correct content. The UE shall include the following lines in the SDP body:

- All mandatory SDP lines are present; and
- "o" line like in INVITE request, except that the version number shall be incremented by one compared to the previously sent SDP offer; and
- SDP must contain at least as many media description lines as the SDP in the INVITE contained.
- The "a=" lines for preconditions in the UPDATE shall be like for INVITE in step 1 but with the following exceptions:
    - in attribute line a=curr:qos local the direction-tag must have the same value that the direction-tag has in the attribute line a=des:qos mandatory local, to indicate that the UE has met its local preconditions.
    - in attribute line a=des:qos [strength-tag] remote [direction-tag] the strength-tag must be "mandatory" (according to what SS answered in 183 response)
- either a=sendonly, a=recvonly or a=sendrecv line. The directionality indicated by this line must be the same as indicated by the a=curr:qos local line for preconditions

...

Step 9: the UE shall send a PRACK request with the correct content, according to common message definitions.

...

Step 12: the UE shall send an ACK request with the correct content, according to common message definitions.

Step 13: the UE shall send a BYE request with the correct content, according to common message definitions.

12.2 MO Call – 503 Service Unavailable

12.2.1 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. The test case is applicable for IMS security or early IMS security.

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.

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 5.1.3.1, 3GPP TR 33.978[59], clause 6.2.3.1.

12.2.3 Test purpose

To verify that when the UE receives a 503 (Service Unavailable) response to an initial INVITE 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.

12.2.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

For value of T see specific message content for 503 (Service Unavailable) message.

1) MO call is initiated on the UE. SS waits for 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

2) The SS responds with a provisional 100 (Trying) response to the INVITE request followed by a 503 (Service Unavailable) response with the Retry-After header set to T.

3) The SS waits for the UE to send an ACK to acknowledge the reception of the 503 (Service Unavailable) response.

4) 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.

5) The UE may reattempt sending the INVITE request after time T.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	The UE sends an INVITE request with the first SDP offer indicating all desired medias and codecs the UE supports
2a	←		100 Trying	The SS responds with a 100 Trying provisional response
2b	←		503 Service Unavailable	Including Retry-After header with period set to T
3	→		ACK	The UE acknowledges the reception of the 503 (Service Unavailable) response
4				The SS waits for a duration of time T and checks that the UE does not re-send the INVITE request
5	→		INVITE	Optional

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 MO call setup' in annex A.2.1.

100 Trying (Step 2a)

Use the default message '100 Trying for INVITE' in annex A.2.2.

503 Service Unavailable (Step 2b)

Use the default message '503 Service Unavailable' in annex A.4.2.

ACK (Step 3)

Use the default message 'ACK' in annex A.2.7.

INVITE (Step 4)

Use the default message 'INVITE for MO call setup' in annex A.2.1.

12.2.5 Test requirements

At step 4 the UE shall not reattempt the INVITE request before time T from the time the SS receives the ACK from the UE in step 2b.

12.3 Void

12.4 MT Call (resource reservation, preconditions used)

12.4.1 Definition

Test to verify that the UE can correctly receive a call initiation request and generate the correct response when using preconditions. This process is described in 3GPP TS 24.229 [10], clause 5.1.4.1. The test case is applicable for IMS security or early IMS security.

12.4.2 Conformance requirement

When the UE sends any response, the UE shall:

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 and the additional requirements contained within RFC 3325 .

The UE shall insert a P-Access-Network-Info header 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. The UE shall populate the P-Access-Network-Info header with its current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4).

...

The precondition 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 as updated by RFC 4032, 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 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

b) the received INVITE request does not include the "precondition" option-tag in the Supported header or Require header 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 and

   - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; 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 or Require header, 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, 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.

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, it shall send the 180 (Ringing) response reliably. 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.

…

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, 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.

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 modifer 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 2833.

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.

If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 and RFC 3311.

…

Upon receipt of an initial SDP offer in which no precondition information is available, the terminating UE shall in the SDP answer:

- if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams in the SDP answer to
  - active mode, if the offered media streams were not listed as inactive; or
  - inactive mode, if the offered media streams were listed as inactive.

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 initial SDP offer (which included one or more media lines which was offered with several codecs) the terminating UE shall select exactly one codec per payload and indicate only the selected codec for the related media stream.

NOTE 1: A SDP media line can indicate several different payloads. For example a media line indicating an audio media type can indicate several codecs for the audio stream as well as the MIME subtype "telephone-event" for DTMF payload.

Upon sending a SDP answer to an initial 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 indicates its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

NOTE 2: If the terminating UE does not support the precondition mechanism it will ignore any precondition information received from the originating UE.

Upon receipt an initial INVITE request, that includes the SDP offer containing an IP address type (in the "c=" parameter) that is not supported by the UE, it shall respond with the 488 (Not Acceptable Here) response with 301 Warning header indicating "incompatible network address format".

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], clauses 5.1.2A.2, 5.1.4.1, 6.1.1 and 6.1.3, 3GPP TR 33.978[59], clause 6.2.3.1.

12.4.3 Test purpose

1) To verify that after receiving a valid INVITE for call initiation, the UE correctly generates and sends the first 183 Session Progress response; and

2) To verify that the UE includes the proper SDP answer to the SDP offer in the INVITE; and

3) To verify that the UE inserts a P-Access-Network-Info header 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. The UE shall populate the P-Access-Network-Info header with its current point of attachment to the IP-CAN as specified for the access network technology ; and

4) To verify that the UE includes the protected server port in any Contact header; and

5) To verify that the UE does not encrypt the SDP payload; and

6) To verify that the UE supports and handles the precondition extension properly

7) To verify that the UE can release the call on receiving BYE from the SS

12.4.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

<The SS is preconfigured to generate SDP offers that are compatible with the UE"s capabilities.>

IMS security (Yes/No)

Early IMS security (Yes/No)

Support for initiating a session (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

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 183 Session Progress from the UE.

4) SS sends PRACK to the UE to acknowledge the 183 Session Progress.

5) SS expects and receives 200OK 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 expects and receives 200OK for UPDATE from the UE, with proper SDP as answer.

8) SS expects and receives 180 Ringing from the UE.

9) SS sends PRACK to the UE to acknowledge the 180 Ringing.

10) SS expects and receives 200OK for PRACK from the UE.

11) SS expects and receives 200OK for INVITE from the UE.

12) SS sends ACK to the UE.

13) SS sends BYE to the UE.

14) SS expects and receives 200OK 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	→		183 Session Progress	The UE sends 183 response reliably with the SDP answer to the offer in INVITE
4	←		PRACK	SS acknowledges the receipt of 183 from the UE. No SDP offer is included here.
5	→		200OK	The UE responds to PRACK with 200OK.
6	←		UPDATE	SS sends an UPDATE with a second SDP offer after having reserved the resources.
7	→		200OK	The UE acknowledges the UPDATE with 200OK 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.
9	←		PRACK	The SS acknowledges the 180 response with PRACK.
10	→		200OK	The UE acknowledges the PRACK with 200OK.
11	→		200OK	The UE responds to INVITE with 200 OK final response after the user answers the call.
12	←		ACK	The SS acknowledges the receipt of 200OK for INVITE.
13	←		BYE	The SS sends BYE to release the call.
14	→		200OK	The UE sends 200OK 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:

Headers to be included	Value/Remark
Supported	
option-tag	*precondition*
SDP	The SDP contains all mandatory SDP lines, as specified in SDP grammar in RFC 4566[27], including: - 'v= 0' - "o=" line indicating e.g. the session identifier and the IP address of the SS; - 's=IMS conformance test' - 't=0 0' - "c=" line indicating the IP address of the SS for receiving the media flow; The SDP includes one or more media description lines based on preconfigured information so that the SDP is compatible with the UE"s capabilities. For each type of offered media the following lines must exist within the SDP: - "m=" line describing the media type, transport port and protocol used for media and media format; - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media; if the media line in the SDP indicates 'video' or 'audio' that utilize the RTP/RTCP - two "b=" lines proposing the bandwidth allocations for RTCP (for "RS" and "RR" modifiers), if the media line in the SDP indicates the usage of RTP/RTCP, as described in RFC 3556[53]; - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line. - Any of the "a=" line for rtpmap attribute may be followed by extra "a=" line for fmtp attribute to convey parameters specific to a particular format; - "a=inactive" line; For each offered media, the precondition shall be set as follows: a=curr:qos local none a=curr:qos remote none a=des:qos mandatory local [direction-tag] (note 1) a=des:qos mandatory remote [direction-tag] (note 2) note 1: The value of direction-tag may be sendrecv, send, or recv. It is preconfigured based on the UE"s capability. note 2: The value of direction-tag may be sendrecv, send, or recv.

100 Trying (Step 2)

Use the default message "100 Trying for INVITE" in annex A2.2.

183 Session Progress (Step 3)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Headers to be included	Value/Remark
Status-Line	
Reason-Phrase	Not checked
Require	
option-tag	*precondition*
SDP	Properly generated 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. For each media, the precondition attribute lines are set as follows: a=curr:qos local [direction-tag] (note 1) a=curr:qos remote none a=des:qos mandatory local [direction-tag] (note 2) a=des:qos mandatory remote [direction-tag] (note 3) a=conf:qos remote [direction-tag] (note 4) a=inactive For each media, the UE shall indicate only one codec. note 1: The current qos status for local may be either none or the inverse of the desired remote value in Step 1 depending on whether the UE"s precondition status has been met. note 2: The inverse of the desired remote value in Step 1. note 3: The inverse of the desired local value in Step 1. note 4: The inverse of the desired local value in Step 1.

PRACK (step 4)

Use the default message "PRACK" in annex A.2.4, but without 'Route' and 'P-Access-Network-Info' headers. 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 with following exceptions:

Headers to be included	Value/Remark
P-Access-Network-Info	same value as in 183 message

UPDATE (step 6)

Use the default message "UPDATE" in annex A.2.5, but without including 'Route', 'Require', 'Proxy-Require', 'Security-Verify', and 'P-Access-Network-Info' headers and with the following exceptions:

Headers to be included	Value/Remark
SDP	Same SDP offer as in INVITE with version number in the 'o' line incremented by one. For each media, the precondition attributes are set as follows: a=curr:qos local [direction-tag] (note 1) a=curr:qos remote [direction-tag] (note 2) a=des:qos mandatory local [direction-tag] (note 3) a=des:qos mandatory remote [direction-tag] (note 4) a=sendonly|recvonly|sendrecv note 1: The same value as the desired local value in Step 1. note 2: The inverse of the current local value in Step 3. note 3: The same value as the desired local value in Step 1. note 4: The same value as the desired remote value in Step 1.

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:

Headers to be included	Value/Remark
SDP	Same SDP answer as in 183 with version number in the 'o' line incremented by one. For each media, the precondition attributes are set as follows: a=curr:qos local [direction-tag] (note 1) a=curr:qos remote [direction-tag] (note 2) a=des:qos mandatory local [direction-tag] (note 3) a=des:qos mandatory remote [direction-tag] (note 4) a=sendonly|recvonly|sendrecv (note 5) note 1: The current qos status for local may be either none or the same as the desired local value in Step 3 depending on whether the UE"s precondition status has been met. note 2: The same value as the desired remote value in Step 3. note 3: The same value as the desired local value in Step 3. note 4: The same value as the desired remote value in Step 3. note 5: The value here shall be the dual of the value in Step 6 (sendonly => recvonly; recvonly => sendonly; sendrecv => sendrecv).
P-Access-Network-Info	same value as in 183 message
Content-Type	application/SDP
Content-Length	length of message body

180 Ringing (step 8)

Use the default message "180 Ringing for INVITE" in annex A.2.6 without the 'Record-Route' header and with the following exceptions:

Headers to be included	Value/Remark
Status-Line Reason-Phrase	 **Not checked**
P-Access-Network-Info	same value as in 183 message
RSeq response-num	 the value in 183 incremented by one

PRACK (step 9)

Use the default message "PRACK" in annex A.2.4, but without 'Route' and 'P-Access-Network-Info' headers. No content body is included in this PRACK message.

200 OK (step 10)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with following exceptions:

Headers to be included	Value/Remark
P-Access-Network-Info	same value as in 183 message

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:

Headers to be included	Value/Remark
P-Access-Network-Info	same value as in 183 message
Record-Route	same value as in INVITE message

ACK (step 12)

Use the default message "ACK" in annex A.2.7 without the 'Route' header.

BYE (step 13)

Use the default message "BYE" in annex A.2.8 without 'Require', 'Proxy-Require', 'Route', 'Security-Verify', and 'P-Access-Network-Info' headers.

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:

Headers to be included	Value/Remark
P-Access-Network-Info	same value as in 183 message

12.4.5 Test requirements

The UE shall send requests and responses described in subclause 12.4.4 over the security association established during the registration/authentication process. The UE shall also include the P-Access-Network-Info header in these messages. If the UE includes Contact header in the request or response, it shall include the protected server port in the Contact header. In addition, if there is SDP content in the SIP message body, the UE shall not encrypt the SDP content.

In step 2, if 100 Trying is sent, the UE shall populate the headers as defined in subclause 12.4.4.

In step 3, the UE shall populate the headers as defined in subclause 12.4.4, and:

1) The UE shall include the answer for the SDP offer in the INVITE. The SDP answer indicates that the UE supports the media type and MIME type offered by the SS.

2) The UE shall request confirmation for the result of the resource reservation at the originating end point. The precondition related SDP lines are verified as described in subclause 12.4.4.

3) The UE shall select exactly one codec per payload and indicate only the selected code for the related media stream.

In step 5, the UE shall populate the headers as defined in subclause 12.4.4.

In step 7, the UE shall populate the headers as defined in subclause 12.4.4 and

- the UE indicates in the SDP answer the precondition status on both ends as described in subclause 12.4.4.

In step 8, the UE shall populate the headers as defined in subclause 12.4.4.

In step 10, the UE shall populate the headers as defined in subclause 12.4.4.

In step 11, the UE shall populate the headers as defined in subclause 12.4.4.

In step 14, the UE shall populate the headers as defined in subclause 12.4.4.

The SS shall check in step 8) that in accordance to the 3GPP TS 24.229[10], the headers covered in the specific message.

12.5 MO Call (resource reservation, preconditions used) against SS (resource reservation, preconditions not used)

12.5.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated call setup and release when it supports and uses preconditions but the terminating UE does not support preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1. The test case is applicable for IMS security and early IMS security.

12.5.2 Conformance requirement

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and
- include the protected server port in any Contact header that is otherwise included.

….

The UE shall insert a P-Access-Network-Info header 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. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

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.

The UE may indicate that proxies should not fork the INVITE request by including a "no-fork" directive within the Request-Disposition header in the initial INVITE request as described in RFC 3841.

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.

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, 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.

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 modifer 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 2833.

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.

If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 and RFC 3311.

An INVITE request generated by a UE shall contain a SDP offer. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP offer with the most preferred codec listed first.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the initial 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.

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 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.

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], clauses 5.1.2A.1, 5.1.3 and 6.1, 3GPP TR 33.978[59], clause 6.2.3.1.

12.5.3 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 falls back to using 'active/ inactive' attributes and basic SIP signalling if the terminating UE does not support preconditions.

4) To verify that the UE is able to release the call.

12.5.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for use of preconditions (Yes/No)

Support for initiating a session which require local and/or remote resource reservation (Yes/No)

UE supports a=inactive (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1) MO call is initiated on the UE. SS waits for 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

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with a 180 Ringing response that does not contain any SDP answer.

4) SS responds to the INVITE request with valid 200 OK response that contains the SDP answer, with the media streams 'active/inactive' mode set according to that received in the INVITE.

5) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

6) If at least one of the offered media streams was listed as inactive in the original INVITE, then steps 6 to 9 are performed; otherwise go directly to Step 10. SS waits for the UE to send reINVITE containing new SDP offer setting the media streams to active mode when resources are ready.

7) SS responds to the reINVITE request with a 100 Trying response.

8) SS responds to the reINVITE request with valid 200 OK response that contains the SDP answer, with the media streams set to active mode.

9) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for reINVITE.

10) Call is released on the UE. SS waits the UE to send a BYE request.

11) SS responds to the BYE request with valid 200 OK response.

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
2	←		100 Trying	The SS responds with a 100 Trying provisional response
3	←		180 Ringing	The SS responds to INVITE with 180 Ringing that does not contain any SDP answer
4	←		200 OK	The SS responds to INVITE with 200 OK and provides the SDP answer with the media streams 'active/inactive' mode set as received in the INVITE
5	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
6	→		reINVITE	Optional step: if at least one of the offered media streams was listed as inactive in the INVITE, UE sends a reINVITE with the media streams set to active mode when resources are ready
7	←		100 Trying	Optional step: the SS responds with a 100 Trying provisional response
8	←		200 OK	Optional step: the SS responds to reINVITE with 200 OK and answers the second SDP offer with the media streams set to active mode
9	→		ACK	Optional step: the UE acknowledges the receipt of 200 OK for reINVITE
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 'IMS security ' or 'early IMS security' when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MO call setup' in annex A.2.1 with the following exceptions. For the contents of the SDP body see test requirement details.

Header/param	Value/remark
Supported	
option-tag	*precondition*

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2.

180 Ringing for INVITE (Step 3)

Use the default message '180 Ringing for INVITE' in annex A.2.6 (for header values in A.2.6 that reference 183 response, the values in A.2.3 shall be used instead), with the following exceptions:

Header/param	Value/remark
Require	This header shall be omitted
Rseq	This header shall be omitted

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	 Same value as in the 180 response
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. The copied SDP body must be modified as follows for the 200 OK response: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should send the media; and - the "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31], shall be omitted. - For each media, include a=sendonly if a=recvonly is received in Step 1; include a=recvonly if a=sendonly is received in Step 1; include a=sendrecv if a=sendrecv is received in Step 1.

ACK (Step 5)

Use the default message 'ACK' in annex A.2.7, with the following exceptions:

Header/param	Value/remark
Request-Line Request-URI	 Same value as in the Contact header in 180 response
Route route-param	 URIs of the Record-Route header of 180 response in reverse order
To Tag	 *Same value as received in the 180 response*

reINVITE (Step 6) Optional step used if 'inactive' attributes were set in the initial SDP offer

Use the default message 'INVITE for MO call setup' in annex A.2.1 with the following exceptions. For the contents of the SDP body see test requirement details.

Header/param	Value/remark
Request-Line	
Request-URI	Same value as the Contact header in 180 in Step 3.
Route	Same value as the header in ACK in Step 5.
From	Same value as the From header in ACK in Step 5.
To	Same value as the To header in ACK in Step 5.
CSeq	
Value	*The value in INVITE in Step 1 incremented by one.*

100 Trying for reINVITE (Step 7) Optional step used if reINVITE was sent at Step 6

Use the default message '100 Trying for INVITE' in annex A.2.2.

200 OK for reINVITE (Step 8) Optional step used if reINVITE was sent at 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
Record-Route	
Rec-route	Same value as in the 180 response
Contact	
Addr-spec	Same value as in the 180 response
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 reINVITE. The copied SDP body must be modified as follows for the 200 OK response: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media. - For each media, include a=sendonly if a=recvonly is received in Step 6; include a=recvonly if a=sendonly is received in Step 6; include a=sendrecv if a=sendrecv is received in Step 6.

ACK (Step 9) Optional step used if reINVITE was sent at Step 6

Use the default message 'ACK' in annex A.2.7, with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	Same value as in the Contact header in 200 response
Route	
route-param	URIs of the Record-Route header of 200 response in reverse order
To	
Tag	*Same value as received in the 200 response*

BYE (Step 10)

Use the default message 'BYE' in annex A.2.8, with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	Same value as in the ACK message
Route	
route-param	Same value as in the ACK message
To	
Tag	Same value as in the ACK message
CSeq	
Value	*The value in INVITE in Step 1 incremented by one if Step 6 is not executed; the value in INVITE in Step 6 incremented by one if Step 6 is executed..*

200 OK for BYE (Step 11)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

12.5.5 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 1: the UE shall send an INVITE message with correct content. The UE shall include the following lines in the SDP body:

- All mandatory SDP lines, as specified in SDP grammar in RFC 4566 [27] appendix A, including:
  - "o=" line indicating e.g. the session identifier and the IP address of the UE;
  - "c=" line indicating the IP address of the UE for receiving the media flow;
- Media description lines for the media proposed by UE for the MO call. For each type of offered media the following lines must exist within the SDP:
  - "m=" line describing the media type, transport port and protocol used for media and media format;
  - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media , however this line may be missing if the media type is something else than "video" or "audio" or the SDP contains "a=sendonly" line, according to RFC 3264 [30];
  - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line:
  - four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31].
    At this stage of the call setup the lines shall be as follows:
    a=curr:qos local [none, send, recv or sendrecv]
    a=curr:qos remote none
    a=des:qos mandatory local [send, recv or sendrecv]
    a=des:qos [none, optional or mandatory] remote [send, recv or sendrecv]
    The direction tag for remote shall be the same as for local. These four "a=" lines may appear in any order.
  - "a=inactive" line if the a=curr:qos local has value none;
  - Optionally the UE can include the "a=[sendonly, recvonly or sendrecv] " line

...

Step 5: the UE shall send an ACK request with the correct content, according to common message definitions.

...

Step 6: the UE may conditionally send a reINVITE request with the correct content. If this request is sent, the UE shall include the following lines in the SDP body:

- All mandatory SDP lines are present; and
- "o" line shall be the same like in INVITE request, except that the version number shall be incremented by one; and
- SDP must contain as many media description lines as the SDP in the INVITE contained; and
- For each type of offered media:
  - the four "a=" lines describing the current and desired state of the preconditions shall be omitted; and
  - the "a=[sendonly, recvonly, or sendrecv] " compatible with the desired direction attributes of the original preconditions in Step 1. For instance, if the original preconditions in Step 1 were:

  a=des:qos mandatory local send
  a=des:qos mandatory remote send

  a valid value in Step 6 would be:

  a= sendonly

...

Step 9: the UE may conditionally send an ACK request with the correct content, according to common message definitions.

...

Step 10: the UE shall send a BYE request with the correct content, according to common message definitions.

12.6 MT Call (resource reservation, preconditions not used)

12.6.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated call setup and release when the UE need to reserve resources but preconditions are not used. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1. The test case is applicable for IMS security or early IMS security.

12.6.2 Conformance requirement

When the UE sends any response, the UE shall:

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP request that is not protected by the security association 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.

…

The UE shall insert a P-Access-Network-Info header 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.

…

The precondition 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 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 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

b) the received INVITE request does not include the "precondition" option-tag in the Supported header or Require header 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 and

  - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; 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 or Require header, the terminating UE shall not make use of the precondition mechanism; or

…

If the terminating UE requires a reliable alerting indication at the originating side, it shall send the 180 (Ringing) response reliably. 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.

…

Upon receipt of an initial SDP offer in which no precondition information is available, the terminating UE shall in the SDP answer:

- if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams in the SDP answer to
  - active mode, if the offered media streams were not listed as inactive; or
  - inactive mode, if the offered media streams were listed as inactive.

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.

…

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], clauses 5.1.2A.2, 5.1.4.1 and 6.1, 3GPP TR 33.978[59], clause 6.2.3.1.

12.6.3 Test purpose

1) To verify that when receiving a MT 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 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.

12.6.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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.

4) SS may send PRACK to the UE to acknowledge the 180 Ringing.

5) SS may receive 200 OK for PRACK from the UE.

6) SS expects and receives 200 OK for INVITE from the UE, with proper SDP as answer.

7) SS send an ACK to acknowledge receipt of the 200 OK for INVITE

8) SS sends a re-INVITE request to the UE with second SDP offer.

9) SS expects and receives 200 OK for INVITE from the UE.

10) SS sends ACK to the UE.

11) SS sends BYE to the UE.

12) 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. The media stream is set to inactive (a=inactive).
2	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
3	→		180 Ringing	(Optional) The UE responds INVITE with 180 Ringing to indicate that the virtual remote UE has started ringing.
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 PRACK with 200 OK.
6	→		200 OK	The UE responds INVITE with 200 OK .
7	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
8	←		INVITE	SS sends INVITE with SDP offer indicating desired medias and codec. The media stream is set to active.
9	→		200 OK	The UE responds INVITE with 200 OK to indicate that the virtual remote UE had answered the call. The media stream is set to active.
10	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
11	←		BYE	The SS releases the call with BYE.
12	→		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
Message-body	The SDP contains all mandatory SDP lines, as specified in SDP grammar in RFC 4566[27], including: - 'v= 0' - "o=" line indicating e.g. the session identifier and the IP address of the SS; - 's=IMS conformance test' - 't=0 0' - "c=" line indicating the IP address of the SS for receiving the media flow; The SDP includes one or more media description lines based on preconfigured information so that the SDP is compatible with the UE"s capabilities. For each type of offered media the following lines must exist within the SDP: - "m=" line describing the media type, transport port and protocol used for media and media format; - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media; if the media line in the SDP indicates 'video' or 'audio' that utilize the RTP/RTCP - two "b=" lines proposing the bandwidth allocations for RTCP (for "RS" and "RR" modifiers), if the media line in the SDP indicates the usage of RTP/RTCP, as described in RFC 3556[53]; - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line. - Any of the "a=" line for rtpmap attribute may be followed by extra "a=" line for fmtp attribute to convey parameters specific to a particular format; - 'a=inactive' line;

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2

180 Ringing (step 3)

Use the default message "180 Ringing for INVITE" in annex A.2.6 without the 'Record-Route' header and with the following exceptions:

Header/param	Value/Remark
Status-Line	
Reason-Phrase	Not checked
P-Access-Network-Info	Not checked
RSeq	Header optional and not checked
Require	Header optional
Message-body	Header optional Contents if present: 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. For the proposed media, the following line must exist: a=[sendonly, recvonly or sendrecv]
Content-Type	Header optional Contents if present: *application/SDP*
Content-Length	Contents if header Content-Type is present: length of message body

PRACK (step 4)

Use the default message "PRACK" in annex A.2.4, but without 'Route' and 'P-Access-Network-Info' headers. No content body is included in this PRACK message.

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
P-Access-Network-Info	Not checked

200 OK for INVITE (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
Message-body	Header optional Contents if present: 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. For the proposed media, the following line must exist: a=[sendonly, recvonly or sendrecv]
P-Access-Network-Info	Not checked
Content-Type	Header optional Contents if present: *application/SDP*
Content-Length	Contents if header Content-Type is present: length of message body

ACK (Step 7)

Use the default message 'ACK' in annex A.2.7 without the 'Route' header.

INVITE (Step 8)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
From	Same value as selected for INVITE in step 1
To addr-spec Tag	 Same value as selected for INVITE in step 1 Same value as received in the 200 OK response in step 6
Call-ID callid	 Same value as selected for INVITE in step 1
CSeq value	 Value of the previous request sent by the SS (either INVITE or PRACK) incremented by one
Message-body	The SDP contains all mandatory SDP lines, as specified in SDP grammar in RFC 4566 [27], including: - 'v= 0' - "o=" line indicating e.g. the session identifier and the IP address of the SS; - 's=IMS conformance test' - 't=0 0' - "c=" line indicating the IP address of the SS for receiving the media flow; The SDP includes one or more media description lines based on preconfigured information so that the SDP is compatible with the UE''s capabilities. For each type of offered media the following lines must exist within the SDP: - "m=" line describing the media type, transport port and protocol used for media and media format; - "b=" line proposing the application specific maximum bandwidth

	("AS" modifier) for the media; if the media line in the SDP indicates 'video' or 'audio' that utilize the RTP/RTCP - two "b=" lines proposing the bandwidth allocations for RTCP (for "RS" and "RR" modifiers), if the media line in the SDP indicates the usage of RTP/RTCP, as described in RFC 3556[53]; - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line. - Any of the "a=" line for rtpmap attribute may be followed by extra "a=" line for fmtp attribute to convey parameters specific to a particular format;

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
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. For the proposed media, the following line must exist: a=[sendonly, recvonly or sendrecv]
P-Access-Network-Info	Not checked
Content-Type	*application/SDP*
Content-Length	length of message body

ACK (step 10)

Use the default message "ACK" in annex A.2.7 without the 'Route' header.

BYE (step 11)

Use the default message "BYE" in annex A.2.8 without 'Require', 'Proxy-Require', 'Route', 'Security-Verify', and 'P-Access-Network-Info' headers.

200 OK (step 12)

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
P-Access-Network-Info	Not checked

12.6.5 Test requirements

The UE shall send requests and responses as described in clause 12.6.4.

The UE shall include the Message-body header with SDP answer in at least one of the step3 or step 6 messages.

12.7 MO Call (no resource reservation, preconditions not used)

12.7.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated call setup and release. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1. The test case is applicable for IMS security or early IMS security.

12.7.2 Conformance requirement

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

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and
- include the protected server port in any Contact header that is otherwise included.

…

The UE shall insert a P-Access-Network-Info header 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. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology.

…

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected server port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

…

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.

…

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.

…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, 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.

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 modifer 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 2833.

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.

…

If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 and RFC 3311.

…

An INVITE request generated by a UE shall contain a SDP offer. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP offer with the most preferred codec listed first.

…

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.…

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], clauses 5.1.2A.1, 5.1.3, 6.1.1 and 6.1.2, 3GPP TR 33.978[59], clause 6.2.3.1.

12.7.3 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 the UE is able to release the call.

12.7.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1) MO call is initiated on the UE. SS waits the UE to send an INVITE request with a SDP offer.

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with valid 200 OK response.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

5) Call is released on the UE. SS waits the UE to send a BYE request.

6) SS responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with a SDP offer
2	←		100 Trying	The SS responds with a 100 Trying provisional response
3	←		200 OK	The SS responds INVITE with 200 OK
4	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
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 'IMS security ' or 'early IMS security' when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MO call setup' in annex A.2.1 For the contents of the SDP body see test requirement details.

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
Record-Route rec-route	 Same value as defined in for Record-Route within clause A2.3. (for 183 response)
Contact addr-spec	 Same value as defined in for Contact within clause A2.3. (for 183 response)
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 but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - optional "a=sendonly" line inverted to "a=recvonly" and vice versa

ACK (Step 4)

Editor's Note: Investigate if the contents of the Route/To parameters should be checked.

Use the default message 'ACK' in annex A.2.7with the following exceptions:

Header/param	Value/remark
Route	Not checked
To	Not checked

BYE (Step 5)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

12.7.5 Test requirements

Step 1: the UE shall send a default message 'INVITE for MO call setup' in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Require	must NOT contain value *precondition*

The UE shall include the following lines in the SDP body:

- All mandatory SDP lines, as specified in SDP grammar in RFC 4566 [27] appendix A, including:
    - "o=" line indicating e.g. the session identifier and the IP address of the UE;
    - "c=" line indicating the IP address of the UE for receiving the media flow;
- Media description lines for the media proposed by UE for the MO call. For each type of offered media the following lines must exist within the SDP:
    - "m=" line describing the media type, transport port and protocol used for media and media format;
    - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media , however this line may be missing if the media type is something else than "video" or "audio" or the SDP contains "a=sendonly" line, according to RFC 3264 [30];
    - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line:

...

Step 4: the UE shall send an ACK request with the correct content, according to common message definitions.

Step 5: the UE shall send a BYE request with the correct content, according to common message definitions.

12.8 MT Call (no resource reservation, preconditions not used)

12.8.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated call setup and release. This process is described in 3GPP TS 24.229 [10], clauses 5.1.4 and 6.1. The test case is applicable for IMS security or early IMS security.

12.8.2 Conformance requirement

When the UE sends any response, the UE shall:

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP request that is not protected by the security association 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.

…

The UE shall insert a P-Access-Network-Info header 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.

…

The precondition 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 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 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

b) the received INVITE request does not include the "precondition" option-tag in the Supported header or Require header 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 and

   - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; 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 or Require header, the terminating UE shall not make use of the precondition mechanism; or

…

If the terminating UE requires a reliable alerting indication at the originating side, it shall send the 180 (Ringing) response reliably. 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.

…

Upon receipt of an initial SDP offer in which no precondition information is available, the terminating UE shall in the SDP answer:

- if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams in the SDP answer to
  - active mode, if the offered media streams were not listed as inactive; or
  - inactive mode, if the offered media streams were listed as inactive.

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.

…

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], clauses 5.1.2A.2, 5.1.4.1 and 6.1, 3GPP TR 33.978[59], clause 6.2.3.1.

12.8.3 Test purpose

1) To verify that when receiving a MT call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that the UE is able to release the call.

12.8.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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.

4) SS may send PRACK to the UE to acknowledge the 180 Ringing.

5) SS may receive 200 OK for PRACK from the UE.

6) SS expects and receives 200 OK for INVITE from the UE, with proper SDP as answer.

7) SS send an ACK to acknowledge receipt of the 200 OK for INVITE

8) SS sends BYE to the UE.

9) 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 after its resource is ready.
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	→		200 OK	The UE responds INVITE with 200 OK .
7	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
8	←		BYE	The SS releases the call with BYE.
9	→		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
Message-body	The SDP contains all mandatory SDP lines, as specified in SDP grammar in RFC 4566[27], including: - 'v= 0' - "o=" line indicating e.g. the session identifier and the IP address of the SS; - 's=IMS conformance test' - 't=0 0' - "c=" line indicating the IP address of the SS for receiving the media flow; The SDP includes one or more media description lines based on preconfigured information so that the SDP is compatible with the UE"s capabilities. For each type of offered media the following lines must exist within the SDP: - "m=" line describing the media type, transport port and protocol used for media and media format; - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media; if the media line in the SDP indicates 'video' or 'audio' that utilize the RTP/RTCP - two "b=" lines proposing the bandwidth allocations for RTCP (for "RS" and "RR" modifiers), if the media line in the SDP indicates the usage of RTP/RTCP, as described in RFC 3556[53]; - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line. - Any of the "a=" line for rtpmap attribute may be followed by extra "a=" line for fmtp attribute to convey parameters specific to a particular format

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2

180 Ringing (step 3)

Use the default message "180 Ringing for INVITE" in annex A.2.6 without the 'Record-Route' header and with the following exceptions:

Header/param	Value/Remark
Status-Line Reason-Phrase	 Not checked
P-Access-Network-Info	Not checked
RSeq	Header optional and not checked
Require	Header optional
Message-body	Header optional Contents if present: 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. For the proposed media, the following line must exist: a=[sendonly, recvonly or sendrecv]
Content-Type	Header optional Contents if present: *application/SDP*
Content-Length	Contents if header Content-Type is present: length of message body

PRACK (step 4)

Use the default message "PRACK" in annex A.2.4, but without 'Route' and 'P-Access-Network-Info' headers. 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 with the following exceptions:

Header/param	Value/remark
P-Access-Network-Info	Not checked

200 OK for INVITE (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
Message-body	Header optional Contents if present: 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. For the proposed media, the following line must exist: a=[sendonly, recvonly or sendrecv]
P-Access-Network-Info	Not checked
Content-Type	Header optional Contents if present: *application/SDP*
Content-Length	Contents if header Content-Type is present: length of message body

ACK (Step 7)

Use the default message 'ACK' in annex A.2.7 without the 'Route' header.

BYE (step 8)

Use the default message "BYE" in annex A.2.8 without 'Require', 'Proxy-Require', 'Route', 'Security-Verify', and 'P-Access-Network-Info' headers.

200 OK (step 9)

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
P-Access-Network-Info	Not checked

12.8.5 Test requirements

The UE shall send requests and responses as described in clause 12.8.4.

The UE shall include the Message-body header with SDP answer in at least one of the step3 or step 6 messages.

12.9 MO Call (no resource reservation, preconditions used)

12.9.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated call setup and release. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1. The test case is applicable for IMS security or early IMS security.

12.9.2 Conformance requirement

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

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and
- include the protected server port in any Contact header that is otherwise included.

…

The UE shall insert a P-Access-Network-Info header 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. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology.

…

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected server port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

…

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.

…

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.

…

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, 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.

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 modifer 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 2833.

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.

…

If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 and RFC 3311.

…

An INVITE request generated by a UE shall contain a SDP offer. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP offer with the most preferred codec listed first.

…

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.

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], clauses 5.1.2A.1, 5.1.3, 6.1.1 and 6.1.2, 3GPP TR 33.978[59], clause 6.2.3.1.

12.9.3 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 the UE is able to release the call.

12.9.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1) MO call is initiated on the UE. SS waits the UE to send an INVITE request with a SDP offer.

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with 180 Ringing response.

4) SS responds to the INVITE request with valid 200 OK response.

5) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

6) Call is released on the UE. SS waits the UE to send a BYE request.

7) SS responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with a SDP offer
2	←		100 Trying	The SS responds with a 100 Trying provisional response
3	←		180 Ringing	The SS responds INVITE with 180 Ringing to indicate that the remote UE has started ringing.
4	←		200 OK	The SS responds INVITE with 200 OK
5	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
6	→		BYE	The UE releases the call with BYE
7	←		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 1)

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 SDP body contains all mandatory SDP lines, as specified in SDP grammar in RFC 4566[27], including: - "o=" line indicating e.g. the session identifier and the IP address of the UE; - "c=" line indicating the IP address of the UE for receiving the media flow; Media description lines for the media proposed by UE for the MO call.For each type of offered media type the following lines must exist within the SDP: - "m=" line describing the media type, transport port and protocol used for media and media format; - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media , however this line may be missing if the media type is something else than "video" or "audio; - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line; - the "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]: 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 2)

Use the default message '100 Trying for INVITE' in annex A.2.2.

180 Ringing for INVITE (Step 3)

Use the default message '180 Ringing for INVITE' in annex A.2.6.

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*
Content-Length Value	 length of message-body
Message-body	SDP body of the 200 response copied from the received INVITE but modified as follows: - IP address on "o=" and "c=" lines 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]: a=curr:qos local sendrecv a=curr:qos remote sendrecv a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv;

ACK (Step 5)

Use the default message 'ACK' in annex A.2.7with the following exceptions:

Header/param	Value/remark
Route	Not checked
To	Not checked

BYE (Step 6)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 7)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

12.9.5 Test requirements

The UE shall send requests and responses as described in clause 12.9.4

12.10 MT Call (no resource reservation, preconditions used)

12.10.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated call setup and release. This process is described in 3GPP TS 24.229 [10], clauses 5.1.4 and 6.1. The test case is applicable for IMS security or early IMS security.

12.10.2 Conformance requirement

When the UE sends any response, the UE shall:

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP request that is not protected by the security association 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.

…

The UE shall insert a P-Access-Network-Info header 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.

…

The precondition 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 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 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

b) the received INVITE request does not include the "precondition" option-tag in the Supported header or Require header 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 and

  - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

  - the required local resources at the originating UE and the terminating UE are available, the terminating UE may use the precondition mechanism;

…

If the terminating UE requires a reliable alerting indication at the originating side, it shall send the 180 (Ringing) response reliably. 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.

…

Upon sending a SDP answer to an initial SDP offer (which included one or more media lines which was offered with several codecs) the terminating UE shall select exactly one codec per payload and indicate only the selected codec for the related media stream.

…

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], clauses 5.1.2A.2, 5.1.4.1 and 6.1, 3GPP TR 33.978[59], clause 6.2.3.1.

12.10.3 Test purpose

1) To verify that when receiving a MT call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that the UE is able to release the call.

12.10.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

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.
4) SS may send PRACK to the UE to acknowledge the 180 Ringing.
5) SS may receive 200 OK for PRACK from the UE.
6) SS expects and receives 200 OK for INVITE from the UE, with proper SDP as answer.
7) SS send an ACK to acknowledge receipt of the 200 OK for INVITE
8) SS sends BYE to the UE.
9) 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.
4	←		PRACK	(Optional) SS shall send PRACK if the 180 response contains 100rel option in the Require header.
5	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
6	→		200 OK	The UE responds INVITE with 200 OK .
7	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
8	←		BYE	The SS releases the call with BYE.
9	→		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 SDP body contains all mandatory SDP lines, as specified in SDP grammar in RFC 4566[27], including: - 'v= 0' - "o=" line indicating e.g. the session identifier and the IP address of the SS; - 's=IMS conformance test' - 't=0 0' - "c=" line indicating the IP address of the SS for receiving the media flow; The SDP includes one media description line based on preconfigured information so that the SDP is compatible with the UE"s capabilities. For the media type the following lines must exist within the SDP: - "m=" line describing the media type, transport port and protocol used for media and media format; - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media; if the media line in the SDP indicates 'video' or 'audio' that utilize the RTP/RTCP - two "b=" lines proposing the bandwidth allocations for RTCP (for "RS" and "RR" modifiers), if the media line in the SDP indicates the usage of RTP/RTCP, as described in RFC 3556[53]; - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line. - Any of the "a=" line for rtpmap attribute may be followed by extra "a=" line for fmtp attribute to convey parameters specific to a particular format; - the "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]: 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 2)

Use the default message '100 Trying for INVITE' in annex A.2.21

80 Ringing for INVITE (step 3)

Use the default message "180 Ringing for INVITE" in annex A.2.6 without the 'Record-Route' header and with the following exceptions:

Header/param	Value/Remark
Status-Line Reason-Phrase	 Not checked
P-Access-Network-Info	Not checked
RSeq	Header optional and not checked
Require	Header optional
Message-body	Header optional Contents if present: 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. For the proposed media, the following line must exist: a=[sendonly, recvonly or sendrecv]
Content-Type	Header optional Contents if present: *application/SDP*
Content-Length	Contents if header Content-Type is present: length of message body

PRACK (step 4)

Use the default message "PRACK" in annex A.2.4, but without 'Route' and 'P-Access-Network-Info' headers. 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 with the following exceptions:

Header/param	Value/remark
P-Access-Network-Info	Not checked

200 OK for INVITE (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
Message-body	Header optional Contents if present: 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. For the proposed media, the following line must exist: a=[sendonly, recvonly or sendrecv]
P-Access-Network-Info	Not checked
Content-Type	Header optional Contents if present: *application/SDP*
Content-Length	Contents if header Content-Type is present: length of message body

ACK (Step 7)

Use the default message 'ACK' in annex A.2.7

BYE (step 8)

Use the default message "BYE" in annex A.2.8 without 'Require', 'Proxy-Require', 'Route', 'Security-Verify', and 'P-Access-Network-Info' headers.

200 OK (step 9)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with following exceptions:

Headers to be included	Value/Remark
P-Access-Network-Info	Not checked

12.10.5 Test requirements

The UE shall send requests and responses as described in clause 12.10.4.

The UE shall include the Message-body header with SDP answer in at least one of the step3 or step 6 messages.

12.11 MO Call (resource reservation, preconditions used)

12.11.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated call setup and release when using preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1. The test case is applicable for IMS security or early IMS security.

12.11.2 Conformance requirement

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and

- include the protected server port in any Contact header that is otherwise included.

….

The UE shall insert a P-Access-Network-Info header 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. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

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 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.

The UE may indicate that proxies should not fork the INVITE request by including a "no-fork" directive within the Request-Disposition header in the initial INVITE request as described in RFC 3841 [56B].

NOTE 3: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. 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 [27]) and does not support the UPDATE request (as described in RFC 3311 [29]).

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.

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].

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[26].

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, 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 [56] to specify the required bandwidth allocation for RTCP.

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 [13].

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifer 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 2833 [23].

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 [54] 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.

If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 [26] and RFC 3311 [29].

An INVITE request generated by a UE shall contain a SDP offer. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP offer with the most preferred codec listed first.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the initial 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 [30] and RFC 4032[64], 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 [39].

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

[30] and RFC 4032[64], 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 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.

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], clauses 5.1.2A.1, 5.1.3 and 6.1, 3GPP TR 33.978[59], clause 6.2.3.1.

12.11.3 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.

12.11.4 Method of test

The method of test shall equal to that described in clause 12.1.4 but with the exceptions described here.

Test procedure

3) SS responds to the INVITE request with a 183 Session in Progress response if the UE did not indicate to have met its local preconditions in step 1 (by adding SDP line a=curr:qos local none).

4) If the SS sent the 183 reponse, SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

5) SS responds to the PRACK request (if UE sent one) with valid 200 OK response.

Expected sequence

Step	**Direction**		**Message**	**Comment**
	UE	**SS**		
3	←		183 Session in Progress	Optional step: The SS responds with an SDP answer indicating the medias and codecs acceptable for SS if the UE has not yet reserved its local resources.
4	→		PRACK	Optional step
5	←		200 OK	Optional step
8	←		180 Ringing	If the UE has already met the preconditions in the INVITE (so that the steps 3 - 7 will be skipped), the SS responds with an SDP answer indicating the media and codecs acceptable to the SS and also indicates that it has reserved the resources.

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MO call setup' in annex A.2.1 with the exception that Supported header shall contain the "precondition" tag.

PRACK (Step 4), optional step used if 183 is sent in step 3

Use the default message 'PRACK' in annex A.2.4 with the exception that either Supported header shall contain the "precondition" tag.

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 exception that either Supported header shall contain the "precondition" tag.

180 Ringing for INVITE (Step 8)

If Step 3~7 are skipped, then the 180 message shall also have the following exceptions:

Header/param	Value/remark
Require	
option-tag	*precondition*
Message-body	SDP body copied from the received INVITE but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - optional "a=sendonly" line inverted to "a=recvonly" and vice versa - the "a=" lines describing the current and desired state of the preconditions, updated as follows: a=curr:qos local [direction-tag] (* a=curr:qos remote [direction-tag] (* a=des:qos mandatory local [direction-tag] (* a=des:qos mandatory remote [direction-tag] (* *) The value of direction-tags in this message must be the inverse from those of INVITE (both a= lines for local and remote). If the INVITE contained the direction-tag as "recv" this message must have it as "send" and vice versa. The value "sendrecv" will be kept as is. The value for direction tag of des:qos remote must be the same as for local. The value for direction tag of curr:qos local and remote must be the inverse of direction tag of curr:qos local within the INVITE.

PRACK (Step 9)

Use the default message 'PRACK' in annex A.2.4. with the following exception:

Header/param	Value/remark
Cseq	
value	- if Steps 3-7 did not take place: value as in reliable response incremented by one. - if Steps 3-5 took place and Steps 6-7 did not take place: value as in PRACK from Step 4 incremented by one. - If Steps 3-7 took place: value as in UPDATE from Step 6 incremented by one.

12.11.5 Test requirements

The test requirements shall equal to that described in clause 12.1.5 but with the exceptions described here.

Step 1: the following lines shall be included in the SDP body of the INVITE:

- For each media description line the UE must add an "a=inactive" line if the a=curr:qos local has value none, and otherwise add either a=sendonly, a=recvonly or a=sendrecv line. The directionality indicated by this line must be the same as indicated by the a=curr:qos local line for preconditions

...

Step 4: the following lines shall be included in the SDP body of PRACK:

- if the UE has met its local preconditions the a=inactive line must be replaced with a=sendonly, a=recvonly or a=sendrecv line. The directionality indicated by this line must be the same as indicated by the a=curr:qos local line for preconditions

...

Step 6: the following lines shall be included in the SDP body of UPDATE:

- when the UE has met its local preconditions the a=inactive line must be replaced with a=sendonly, a=recvonly or a=sendrecv line. The directionality indicated by this line must be the same as indicated by the a=curr:qos local line for preconditions

13 Signalling Compression (SIGComp)

13.1 SigComp in the Initial registration

13.1.1 Definition and applicability

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. The test case is applicable for IMS security.

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 notifiaction 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 implicitely by checking the messages sent by the UEverifing the correct exchange of SIP protocol signalling messages.

NOTE: The presence of the SIP Compression announcement 'comp=sigcomp' by either 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].

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

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

13.2.1 Definition and applicability

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 either 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.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for use of preconditions (Yes/No)

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

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

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 with the following exceptions:

Header/param	Value/remark
Via via-parm	 Same value as in the 180 response
Record-Route rec-route	 Same value as in the 180 response
Contact addr-spec	 Same value as in the 180 response

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

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

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

13.3.1 Definition and applicability

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 either 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.

Related ICS/IXIT Statement(s)

The SS is preconfigured to generate SDP offers that are compatible with the UE''s capabilities

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 (optional)
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	The Compression parameter is included in the first route parameter
compression-param	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
Route	
route-param	Not Present
P-Access-Network-Info	
access-net-spec	Not Present
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 with following exceptions:

Header/param	Value/remark
P-Access-Network-Info	
access-net-spec	Same value as in 183 message

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)
Route route-param	 Not Present
Require sec-agree **Proxy-Require** option-tag	 Not Present Not Present
Security-Verify sec-mechanism	 Not Present
P-Access-Network-Info access-net-spec	 Not Present
Message-body	Same SDP offer as in INVITE with version number in the 'o' line incremented by one. 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
P-Access-Network-Info access-net-spec	 Same value as in 183 message
Content-Type media-type	 application/SDP
Message-body	Same SDP answer as in 183 with version number in the 'o' line incremented by one. 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
Record-Route route-param	 Not Present
P-Access-Network-Info access-net-spec	 same value as in 183 message
RSeq response-num	 the value in 183 incremented by one
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
Route	
route-param	Not Present
P-Access-Network-Info	
access-net-spec	Not Present
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 with following exceptions:

Header/param	Value/remark
P-Access-Network-Info	
access-net-spec	same value as in 183 message

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
Record-Route	
route-param	same value as in INVITE message
P-Access-Network-Info	
access-net-spec	same value as in 183 message
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
Route	
route-param	Not Present

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
Route route-param	 Not Present
Require option-tag	 Not Present
Proxy-Require option-tag	 Not Present
Security-Verify sec-mechanism	 Not Present
P-Access-Network-Info access-net-spec	 Not Present

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
P-Access-Network-Info access-net-spec	 same value as in 183 message
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 Invalid Behaviour - State creation before authentication

13.4.1 Definition and applicability

Test to verify that when the P-CSCF tries to create a state in the SigComp State handler before the SA the UE does not create.

13.4.2 Conformance requirement

The UE shall support SigComp as specified in RFC 3320 [24]. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486 [26]. When the UE will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations are set up. The compartment shall finish when the UE is deregistered. State creations and announcements shall be allowed only for messages received in a security association.

NOTE: Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

Reference(s)

3GPP TS 24.229[10], clause 8.1.1.

13.4.3 Test purpose

To verify that, when the P-CSCF try to create a state with the first REGISTER request in th UE state handler the UE does not create it.

NOTE: The RFC 3320 [26] in the clause 10 (Security Considerations) point out the attention on the Integrity risk because the SigComp approach assumes that there is appropriate integrity protection below and/or above the SigComp layer, for this reason is not acceptable that state can be created outside security association.

13.4.4 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.

Related ICS/IXIT Statement(s)

- UE indicating its willingness to receive the responses and requests compressed from initial REGISTER onwards by using the "comp=sigcomp" parameter (Yes/No)

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 shall 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. The SigComp uploaded UDVM bytecode contains an instruction for the creation of new state with the intention to cause a Decompression Failure in the UE.

NOTE: If a decompression failure occurs when decompressing a message in general a dispatcher should discard the compressed message (or the compressed stream if the transport is stream-based) and any decompressed data that has been outputted but not yet passed to the application.

3) After the UE client time out expiry the SS waits for the UE sends another initial REGISTER request. This means that the message in the Step 2 has caused a Decompression Failure in the UE. The SIP Compression announcement 'comp=sigcomp' in the Via header and in the Contact shall be included. The message can be sent compressed or not compressed.

4) 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.

5) 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 shall be included. The message can be sent compressed or not compressed.

6) 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.

7) 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 shall be included. The message can be sent compressed or not compressed.

8) 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.

9) 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.

10) 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 SigComp uploaded UDVM bytecode contains an instruction for the creation of new state with the intention to cause a Decompression Failure in the UE
3	→		REGISTER	After the UE client time out expiry he SS waits for the UE sends another initial REGISTER request. This means that the message in the Step 2 has caused a Decompression Failure in the UE
4	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network. This message is sent compressed.
5	→		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.
6	←		200 OK	The SS responds with 200 OK. This message is sent compressed.
7	→		SUBSCRIBE	The UE subscribes to its registration event package. The message can be sent compressed or not compressed.
8	←		200 OK	The SS responds with 200 OK. This message is sent compressed.
9	←		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.
10	→		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 shall be used to indicate that 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. This message contains in the SigComp Layer an appropriate UDVM instruction for state creation.

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1, condition A1 "Initial unprotected REGISTER". The following exceptions shall be used to indicate that 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 4)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2.

REGISTER (Step 5)

Use the default message 'REGISTER' in annex A.1.1, condition A2 "Subsequent REGISTER sent over security associations". The following exceptions shall be used to indicate that 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 6)

Use the default message '200 OK for REGISTER' in annex A.1.3.

SUBSCRIBE (Step 7)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4. The following exceptions shall be used to indicate 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 8)

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 9)

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 10)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

13.4.5 Test requirements

Step 3: The SS shall check that after client time-out expiry in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends another initial REGISTER request as in Step 1, this means that the message in the Step 2 has caused a Decompression Failure

14 Emergency Service

14.1 Emergency Call Initiation – Using CS domain

14.1.1 Definition and applicability

Test to verify that the UE correctly requests an emergency service on the CS domain. This process is described in 3GPP TS 24.229 [10], clauses 5.1.6. The test case is applicable for IMS security or early IMS security.

14.1.2 Conformance requirement

If the UE does recognise the emergency call MMI(s) (i.e. the dialled number is stored in USIM/ME), then the UE shall use the CS CN domain to attempt to establish the emergency call.

A UE shall not attempt to establish an emergency session via the IM CN Subsystem when the UE can detect that the number dialled is an emergency number. The UE shall use the CS domain as described in 3GPP TS 24.008.

As a consequence of this, a UE operating in MS operation mode C cannot perform emergency calls.

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], clauses 5.16.

3GPP TS 22.101[39], clause 10.4.

3GPP TR 33.978[59], clause 6.2.3.1.

14.1.3 Test purpose

To verify that when calling an emergency number the UE attempts an emergency call setup according to the procedures described in 3GPP TS 24.008 [12].

14.1.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), 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 (early IMS security 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).

Related ICS/IXIT Statement(s)

UE supports Emergency speech call (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1) MO call is initiated on the UE by dialling emergency number, e.g. 112.

2) SS waits for an emergency call setup according to the procedures described in 3GPP TS 24.008 [12].

3) Having reached the active state, the call is cleared by the SS.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				MO call is initiated on the UE by dialling emergency number, e.g. 112. The dialled number shall be one programmed in test USIM EF_{ECC} (Emergency Call Codes), ref. 34.108 [40] clause 8.3.2.21.
2				SS waits for an emergency call setup according to the procedures described in 3GPP TS 24.008[12]
3				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 'early IMS security' when applicable

Specific Message Contents

None

14.1.5 Test requirements

Step 2, 3: SS must check that the emergency call on the CS domain is successfully established according to the procedures described in 3GPP TS 24.008 [12].

14.2 Emergency Call Initiation – 380 Alternative Service

14.2.1 Definition and applicability

Test to verify that the UE correctly requests an emergency service on CS domain if the UE has received a 380 (Alternative Service) response to an INVITE request. This process is described in 3GPP TS 24.229 [10], clauses 5.1.6. The test case is applicable for IMS security or early IMS security.

14.2.2 Conformance requirement

If the UE does not recognise the emergency call MMI(s) (i.e. the dialled number is not stored in USIM/ME) but the serving network recognises the dialled number as an emergency call number used in the country then the IM CN subsystem shall inform the UE to use a CS CN domain for emergency services.

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> element with the <type> child element set to "emergency", the UE shall automatically:

- send an ACK request to the P-CSCF as per normal SIP procedures;
- attempt an emergency call setup according to the procedures described in 3GPP TS 24.008.

The UE may also provide an indication to the user based on the text string contained in the <reason> element.

As a consequence of this, a UE operating in MS operation mode C cannot perform emergency calls.

Reference(s)

3GPP TS 24.229[10], clauses 5.16.

3GPP TS 22.101[39], clause 10.4.

14.2.3 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> element with the <type> child element set to "emergency", the UE:
    - send an ACK request to the P-CSCF as per normal SIP procedures;
    - attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [12].

14.2.4 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 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.

Related ICS/IXIT Statement(s)

UE supports Emergency speech call (Yes/No)

UE capable of initiating a bidirectional voice session over IMS (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1) MO call is initiated on the UE by dialling a non emergency number.
2) SS waits the UE to send an INVITE request with Request-URI that matches the non emergency number dialled.
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) SS waits for an emergency call setup according to the procedures described in 3GPP TS 24.008 [12].
6) Having reached the active state, the call is cleared by the SS.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				MO call is initiated on the UE by dialling a 'non emergency' number. The dialled number shall not be one programmed in test USIM field EF_{ECC} (Emergency Call Codes), ref. 34.108[40] clause 8.3.2.21.
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 3GPP TS 24.008[12]
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 'early IMS security' when applicable.Specific Message Contents

INVITE (Step 2)

Use the default message 'INVITE' in annex A.2.1.

380 Alternative Service (Step 3)

Use the default message '380 Alternative Service' in annex A.4.1.

ACK (Step 4)

Header/param	Value/remark	Rel	Reference
Request-Line			RFC 3261 [15]
Method	*ACK*		
Request-URI	same value as received in INVITE message		
SIP-Version	*SIP/2.0*		
Via			RFC 3261 [15]
via-parm	same value as received in INVITE message		
Route			RFC 3261 [15]
route-param	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	same value as received in 380 message		
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		
method	*ACK*		
Max-Forwards			RFC 3261 [15]
value	non-zero value		
P-Access-Network-Info	must **not** be present		RFC 3455 [18]
Content-Length			RFC 3261 [15]
value	0		

14.2.5 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 2: the UE sends an INVITE message with correct content.

Step 4: the UE shall send an ACK.

Step 5, 6: SS must check that the emergency call on the CS domain is successfully established according to the procedures described in 3GPP TS 24.008 [12].

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 and Record-Route headers) where the order is important.

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.

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.

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 px_HomeDomainName (when using ISIM) or SIP URI formed from home domain name derived from px_IMSI (when using USIM)		
SIP-Version		*SIP/2.0*		
Route		**(if present)**		RFC 3261 [15]
route-param	A1, A3	<*sip*:px_pcscf;*lr*>		
route-param	A2	<*sip*:px_pcscf:protected server port of P-CSCF;*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, A3	IP address or FQDN and indicate an unprotected server port of the UE. Port number may be omitted if the request was sent from port 5060.		
sent-by	A2	IP address or FQDN and protected server port of the UE		
via-branch		value starting with "*z9hG4bk*"		
From				RFC 3261 [15]
addr-spec	A1, A2	px_PublicUserIdentity (when using ISIM) or public user identity derived from px_IMSI (when using USIM)		
addr-spec	A3	public user identity derived from px_IMSI		
tag		must be present, value not checked		
To				RFC 3261 [15]
addr-spec	A1, A2	px_PublicUserIdentity (when using ISIM) or public user identity derived from px_IMSI (when using USIM)		
addr-spec	A3	public user identity derived from px_IMSI		
tag		must not be present		
Contact				RFC 3261 [15]
addr-spec	A1, A3	SIP URI to either indicate an unprotected port selected by the UE or no port at all		
addr-spec	A2	SIP URI with IP address or FQDN and protected server port of UE		
expires		*600000* (if present, see Rule 1)		
Expires		**(if present, see Rule 1)**		RFC 3261 [15]
delta-seconds		*600000*		
Require	A1, A2			RFC 3261 [15] RFC 3329 [21]
option-tag		*sec-agree*		
Proxy-Require	A1, A2			RFC 3261 [15] RFC 3329 [21]
option-tag		*sec-agree*		
Supported				RFC 3261 [15]
option-tag		*path*		
CSeq				RFC 3261 [15]
value	A1, A3	must be present, value not checked		
value	A2	must be incremented from the previous REGISTER		
method		*REGISTER*		
Call-ID				RFC 3261 [15]
callid	A1, A3	value not checked		
callid	A2	the same value as in the previous REGISTER		

Header/param	Cond	Value/remark	Rel	Reference
Security-Client	A1, A2			RFC 3329 [21]
mechanism-name		*ipsec-3gpp*		
algorithm		*hmac-md5-96*		
protocol		*esp* (if present)		
mode		*trans* (if present)		
encrypt-algorithm		***des-ede3-cbc*** or ***aes-cbc,*** if UE supports IPSec ESP confidentiality protection ***null*** or parameter not present, if the UE does not support IPSec ESP confidentiality protection		
spi-c		SPI number of the inbound SA at the protected client port		
spi-s		SPI number of the inbound SA at the protected server port		
port-c		protected client port		
port-s		protected server port		
mechanism-name		*ipsec-3gpp*		
algorithm		*hmac-sha-1-96*		
protocol		*esp* (if present)		
mode		*trans* (if present)		
encrypt-algorithm		***des-ede3-cbc*** or ***aes-cbc,*** if UE supports IPSec ESP confidentiality protection ***null*** or parameter not present, if the UE does not support IPSec ESP confidentiality protection		
spi-c		SPI number of the inbound SA at the protected client port		
spi-s		SPI number of the inbound SA at the protected server port		
port-c		protected client port		
port-s		protected server port		
Security-Verify	A2	(not present when A1, A3)		RFC 3329 [21]
sec-mechanism	A2	same value as SecurityServer header sent by SS		
Authorization	A1			RFC 2617 [16]
username	A1	px_PrivateUserIdentity (when using ISIM) or private user identity derived from px_IMSI (when using USIM)		RFC 3310 [17]
realm	A1	px_HomeDomainName (when using ISIM) or home domain name derived from px_IMSI (when using USIM)		
nonce	A1	set to an empty value		
digest-uri	A1	SIP URI formed from px_HomeDomainName (when using ISIM) or formed from home domain name derived from px_IMSI (when using USIM)		
response	A1	set to an empty value		
Authorization	A2			RFC 2617 [16]
username	A2	px_PrivateUserIdentity (when using ISIM) or private user identity derived from px_IMSI (when using USIM)		RFC 3310 [17]
realm	A2	same value as received in the realm directive in the WWW Authenticate header sent by SS		
nonce	A2	same value as in WWW-Authenticate header sent by SS		
opaque	A2	px_Opaque		
digest-uri	A2	SIP URI formed from px_HomeDomainName (when using ISIM) or formed from home domain name derived from px_IMSI (when using USIM)		
qop-value	A2	*auth*		
cnonce-value	A2	value assigned by UE affecting the response calculation		
nonce-count	A2	counter to indicate how many times UE has sent the same value of nonce within successive REGISTERs, initial value shall be 1		
response	A2	response calculated by UE		
algorithm	A2	*AKAv1-MD5*		

Header/param	Cond	Value/remark	Rel	Reference
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A2	(header optional when A1, A3)		RFC 3455 [18]
access-net-spec	A2	access network technology and, if applicable, the cell ID		
Content-Length				RFC 3261 [15]
value		length of request body, if such is present		

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.

Condition	Explanation
A1	Initial unprotected REGISTER (IMS security, A.6a/2)
A2	Subsequent REGISTER sent over security associations (IMS security, A.6a/2)
A3	REGISTER for the case UE supports early IMS security (A.6a/1)

Note1: All choices for applicable conditions are described for each header.

A.1.2 401 Unauthorized for REGISTER

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*401*		
Reason-Phrase	*Unauthorized*		
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	px_ToTagRegister		
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		
WWW-Authenticate			RFC 2617 [16] RFC 3310 [17]
realm	px_HomeDomainName or home domain name derived from px_IMSI NOTE: this value could be set different by the SS (see CP-060230)		
algorithm	*AKAv1-MD5*		
qop-value	*auth*		
nonce	Base 64 encoding of RAND and AUTN		
opaque	px_Opaque		
Security-Server			RFC 3329 [21]
mechanism-name	*ipsec-3gpp*		
algorithm	px_IpSecAlgorithm (hmac-md5-96 or hmac-sha-1-96)		
spi-c	SPI number of the inbound SA at the protected client port		
spi-s	SPI number of the inbound SA at the protected server port		
port-c	px_SSProtectedClientPort		
port-s	px_SSProtectedServerPort		
Encrypt-algorithm	des-ede3-cbc or aes-cbc, if UE supports IPSec ESP confidentiality protection (px_CiphAlgo_Def)		
q	0.9		
Mechanism-name	Ipsec-3gpp		
algorithm	Algorithm not selected by px_IpSecAlgorithm (hmac-sha-1-96 or hmac-md5-96)		
spi-c	SPI number of the inbound SA at the protected client port		
spi-s	SPI number of the inbound SA at the protected server port		
port-c	px_SSProtectedClientPort		
port-s	px_SSProtectedServerPort		
encrypt-algorithm	des-ede3-cbc or aes-cbc, if UE supports IPSec ESP confidentiality protection (px_CiphAlgo_Def)		
q	0.7		
Content-Length			RFC 3261 [15]
value	0		

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		px_ToTagRegister		
From				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
tag		same value as received in REGISTER message		
Call-ID	A1, A2			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]
addr-spec		same value as received in REGISTER message		
expires		px_RegisterExpiration		
P-Associated-URI		order of the parameters in this header must be like in this table		RFC 3455 [18]
addr-spec		px_PublicUserIdentity		
addr-spec		px_AssociatedTelUri any arbitary TEL URI for the user		
Service-Route				RFC 3608 [19]
addr-spec		px_scscf		
uri-parameter		*lr*		
Path				RFC 3327 [20]
addr-spec		px_pcscf		
uri-parameter		*lr*		
Content-Length				RFC 3261 [15]
value		0		

A.1.4 SUBSCRIBE for reg-event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*SUBSCRIBE*		
Request-URI		px_PublicUserIdentity		
SIP-Version		*SIP/2.0*		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
route-param	A1	*<sip:*px_pcscf:protected server port of P-CSCF*;lr>, <sip:*px_scscf*;lr>*		
route-param	A2	*<sip:*px_pcscf: unprotected server port of P-CSCF (optional)*;lr>, <sip:*px_scscf*;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		px_PublicUserIdentity		
tag		must be present, value not checked but stored for later reference		
To				RFC 3261 [15]
addr-spec		px_PublicUserIdentity		
tag		must not be present		
Contact				RFC 3261 [15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of UE		
addr-spec	A2	SIP URI with IP address or FQDN and unprotected server port of UE		
Expires				RFC 3261 [15]
delta-seconds		*600000*		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as SecurityServer 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	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Accept		**(if present)**		RFC 3261 [15]
media-range		*application/reginfo+xml*		RFC 3680 [22]
Event				RFC 3265 [34]
event-type		*Reg*		RFC 3680 [22]
Content-Length				RFC 3261 [15]
value		length of request body, if such is present		

Condition	Explanation
A1 A2	IMS security (A.6a/2) early IMS security (A.6a/1)

Note1: All choices for applicable conditions are described for each header.

A.1.5 200 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		px_PublicUserIdentity		
tag		px_ToTagSubscribeDialog		
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:*px_scscf>		
Expires				RFC 3261 [15]
delta-seconds		600000		
Record-Route				RFC 3261 [15]
addr-spec	A1	px_pcscf: protected server port of SS		
addr-spec	A2	px_pcscf: unprotected server port of SS (optional)		
uri-parameter		*Lr*		
Content-Length				RFC 3261 [15]
value		0		

Condition	Explanation
A1 A2	IMS security (A.6a/2) early IMS security (A.6a/1)

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	SIP URI with IP address or FQDN and protected server port of UE		
Request-URI	A2	SIP URI with IP address or FQDN 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		
sent-by	A2	IP address and unprotected server port of SS (optional)		
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		px_scscf		
via-branch		value starting with "*z9hG4bk"*		
From				RFC 3261 [15]
addr-spec		px_PublicUserIdentity		
tag		px_ToTagSubscribeDialog		
To				RFC 3261 [15]
addr-spec		px_PublicUserIdentity		
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			RFC 3261 [15]
value		1		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec		<*sip:*px_scscf>		
Content-Type				RFC 3261 [15] RFC 3680 [22]
media-type		*application/reginfo+xml*		
Event	A1,A2			RFC 3265[34] RFC 3680 [22]
event-type		*reg*		
Max-Forwards				RFC 3261 [15]
value		*69*		
Subscription-State				RFC 3265[34]
substate-value		*active*		
expires		*600000*		
Content-Length				RFC 3261 [15] RFC 3680 [22]
value		length of message-body		
Message-body		*<?xml version='1.0?>* *<reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='0' state='full'>* *<registration aor=*'px_PublicUserIdentity' *id='a100' state='active'>* *<contact id='980' state='active' event='registered'>* *<uri>*same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>*		

Header/param	Cond	Value/remark	Rel	Reference
		<registration aor='px_AssociatedTelUri' *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>*		

Condition	Explanation
A1	IMS security (A.6a/2)
A2	early IMS security

Note1: All choices for applicable conditions are described for each header.

A.1.7 423 Interval Too Brief for REGISTER

Header/param	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	px_ToTagRegister		
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 from 0 to (2**32)-1)*		

A.1.8 420 Bad Extension for REGISTER

Header/param	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	px_ToTagRegister		
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*		

A.2 Default messages for Call Setup

A.2.1 INVITE for MO Call Setup

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*INVITE*		
Request-URI		px_CalleeUri		
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	<*sip*:px_pcscf:px_SSProtectedServerPort*;lr*>, <*sip*:px_scscf*;lr*>		
	A2	<*sip*:px_pcscf:px_SSUnprotectedServerPort (optional)*;lr*>*, <sip:*px_scscf*;lr*		
From				RFC 3261 [15]
addr-spec		any SIP URI except public user identity derived from px_IMSI		
tag		must be present, value not checked		
To				RFC 3261 [15]
addr-spec		px_CalleeUri		
tag		not present		
Call-ID				RFC 3261 [15]
callid		value different to that received in REGISTER message		
CSeq				RFC 3261 [15]
value		must be present, value not checked		
method		*INVITE*		
Supported				RFC 3261 [15]
option-tag		*100rel*		
Require		(header optional in A2)		RFC 3261 [15] RFC 3312 [31] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Proxy-Require		(header optional in A2)		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Security-Verify	A1	(not present in A2)		RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
Contact				RFC 3261 [15]
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		
Content-Type				RFC 3261 [15]
media-type		*application/sdp*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]

Header/param	Cond	Value/remark	Rel	Reference
access-net-spec		access network technology and, if applicable, the cell ID		
Content-Length				RFC 3261 [15]
Value		length of message-body		

Condition	Explanation
A1	IMS security (A.6a/2)
A2	early IMS security (A.6a/1)

Note1: All choices for applicable conditions are described for each header.

A.2.2 100 Trying for INVITE

Header/param	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	not present		
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.2.3 183 Session in 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 in Progress*		
Record-Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
rec-route	A1,A2	<sip:pcscf.other.com;lr>, <sip:scscf.other.com;lr>, <sip:orig@px_scscf;lr>, <sip:px_pcscf:px_SSProtectedServerPort;lr>		
rec-route	A3,A4	<sip:pcscf.other.com;lr>, <sip:scscf.other.com;lr>, <sip:orig@px_scscf;lr>, <sip:px_pcscf:px_SSUnprotectedServerPort (optional);lr>		
Via				RFC 3261 [15]
via-parm		same value as received in INVITE message		
Require				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		px_InviteToTag		
Contact				RFC 3261 [15]
addr-spec	A1, A3	px_CalleeContactUri		
addr-spec	A2	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		
Rseq				RFC 3262 [33]
response-num		px_RSeqNumFor183		
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		
Allow				RFC 3261 [15]
method		*UPDATE*		
Content-Type				RFC 3261 [15]
media-type		*application/sdp*		
Content-Length				RFC 3261 [15]
value		length of message-body		

Condition	Explanation
A1	MO call setup (IMS security ,A.6a/2)
A2	MT call setup (IMS security ,A.6a/2)
A3	MO call setup (early IMS security, A.6a/1)
A4	MT call setup (early IMS security, A.6a/1)

Note1: All choices for applicable conditions are described for each header.

A.2.4 PRACK

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*PRACK*		
Request-URI		*same value as in Contact header of 183 response*		
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 INVITE message*		
via-branch		value starting with "*z9hG4bk"*		
Route				RFC 3261 [15]
route-param		URIs of the Record-Route header of 183 response in reverse order		
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		same value as in the corresponding reliable response		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		value as in reliable response incremented 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 reliable response		
method		same value as in CSeq of reliable response		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
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	IMS support
A2	early IMS security

A.2.5 UPDATE

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*UPDATE*		
Request-URI		*same value as in PRACK message*		
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 INVITE message*		
via-branch		value starting with "*z9hG4bk*"		
Route				RFC 3261 [15]
route-param		URIs of the Record-Route header of 183 response in reverse order		
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		same value as in 183 message		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		value of received in INVITE incremented by two		
method		*UPDATE*		
Require		(header optional in A2)		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Proxy-Require		(header optional in A2)		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*Sec-agree*		
Max-Forwards				RFC 3261 [15]
value		Non-zero value		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Content-Type				RFC 3261 [15]
media-type		*application/sdp*		
Content-Length				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	IMS security (A.6a/2)
A2	early IMS security (A.6a/1)

Note1: All choices for applicable conditions are described for each header.

A.2.6 180 Ringing for INVITE

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*180*		
Reason-Phrase	*Ringing*		
Record-Route			RFC 3261 [15]
rec-route	same value as in the 183 response		
Via			RFC 3261 [15]
via-parm	same value as in the 183 response		
Require			RFC 3261 [15]
option-tag	*100rel*		
From			RFC 3261 [15]
addr-spec	same value as in the 183 response		
tag	same value as in the 183 response		
To			RFC 3261 [15]
addr-spec	same value as in the 183 response		
tag	same value as in the 183 response		
Contact			RFC 3261 [15]
addr-spec	same value as in the 183 response		
Rseq			RFC 3262 [33]
response-num	px_RSeqNumFor183 incremented by one		
Call-ID			RFC 3261 [15]
callid	same value as in the 183 response		
CSeq			RFC 3261 [15]
value	same value as in the 183 response		
Content-Length			RFC 3261 [15]
value	0		

A.2.7 ACK

Header/param	Value/remark	Rel	Reference
Request-Line			RFC 3261 [15]
Method	*ACK*		
Request-URI	*same value as in PRACK message*		
SIP-Version	*SIP/2.0*		
Via			RFC 3261 [15]
via-parm	same value as received in INVITE message		
Route			RFC 3261 [15]
route-param	URIs of the Record-Route header of 183 response in reverse order		
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	same value as received in 183 message		
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		
method	*ACK*		
Max-Forwards			RFC 3261 [15]
value	non-zero value		
P-Access-Network-Info	must **not** be present		RFC 3455 [18]
Content-Length			RFC 3261 [15]
value	0		

A.2.8 BYE

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*BYE*		
Request-URI		*same value as in PRACK message*		
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 INVITE message*		
via-branch		value starting with "*z9hG4bk"*		
Route				RFC 3261 [15]
route-param		URIs of the Record-Route header of 183 response in reverse order		
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		same value as in the 183 message		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		must be present, not checked		
method		*BYE*		
Require		(header optional in A2)		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Proxy-Require		(header optional in A2)		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
P-Access-Network-Info	A1	(header optional in A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Content-Length				RFC 3261 [15]
value		length of message body		

Condition	Explanation
A1	IMS security (A.6a/2)
A2	early IMS security (A.6a/1)

Note1: All choices for applicable conditions are described for each header.

A.2.9 INVITE for MT Call

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261[15]
Method		*INVITE*		
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* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1	px_pcscf:px_SSProtectedServerPort		
sent-by	A2	IP address or FQDN and unprotected server port of the SS (optional)		
Via-branch		Value starting with "*z9hG4bk"*		
Via		In addition to the via-parm entry for the SS, the following via-parm entries are included:		RFC 3261[15]
via-parm		*SIP/2.0/UDP scscf1.3gpp.org;branch=z9hG4bK1234567890,* *SIP/2.0/UDP scscf2.3gpp.org;branch=z9hG4bK2345678901,* *SIP/2.0/UDP pcscf2.3gpp.org;branch=z9hG4bk3456789012,* *SIP/2.0/UDP caller.3gpp.org:6543;branch=z9hG4bk4567890123*		
Record-Route				RFC 3261[15]
rec-route	A1	<sip:px_pcscf:px_SSProtectedServerPort;lr>		
rec-route	A2	SIP URI with FQDN or IP address and unprotected server port of the SS (optional)		
Record-Route		In addition to the rec-route entry for the SS, the following rec-route entries are included:		RFC 3261[15]
rec-route		*<sip:term@scscf1.3gpp.org;lr>, <sip:orig@scscf2.3gpp.org;lr>, <sip:pcscf2.3gpp.org;lr>*		
From				RFC 3261[15]
addr-spec		an SIP URI representing the calling UE		
Tag		any value (e.g. abc1)		
To				RFC 3261[15]
addr-spec		SIP or TEL URI 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 (e.g. 4711)		
method		*INVITE*		
Supported				RFC 3261[15]
option-tag		*100rel*		
P-Called-Party-ID		One of the UE"s registered, non-barred public ID		RFC 3455[18]
Contact				RFC 3261[15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of the calling UE, for example 'sip:caller@3gpp.org:6543'		
addr-spec	A2	SIP URI with IP address or FQDN and unprotected server port of the calling UE		
Content-Type				RFC 3261[15]
media-type		*application/sdp*		
Max-Forwards				RFC 3261[15]
value		non-zero value		
Content-Length				RFC 3261[15]
value		length of message-body		

Condition	Explanation
A1 A2	IMS security (A.6a/2) early IMS security (A.6a/1)

Note1: All choices for applicable conditions are described for each header.

A.3 Generic Common Messages

A.3.1 200 OK for other requests than REGISTER or SUBSCRIBE

Header/param	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 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	same value as received in request or px_InviteToTag added if missing from request		
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.3.2 403 FORBIDDEN

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*403*		
Reason-Phrase	*Forbidden*		
Via			RFC 3261 [15]
via-parm	same value as received in the previous REGISTER message		
To			RFC 3261 [15]
addr-spec	same value as received in the previous REGISTER message		
tag	px_ToTagRegister		
From			RFC 3261 [15]
addr-spec	same value as received in the previous REGISTER message		
Call-ID			RFC 3261 [15]
value	same value as received in the previous REGISTER message		
CSeq			RFC 3261 [15]
value	same value as received in the previous REGISTER message		
Content-length			RFC 3261 [15]
value	0		RFC 3261 [15]

A.4 Other Default Messages

A.4.1 380 Alternative Service

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*380*		
Reason-Phrase	Alternative Service		
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	same value as received in request or px_InviteToTag 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	Length of the XML body		
XML Message body			TS 24.229 [10], 7.6
<alternative service>			
<type>	Emergency		

A.4.2 503 Service Unavailable

Header/param	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		
Content-Length			RFC 3261 [15]
value	0		
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*		

A.4.3 PUBLISH

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3903 [60]
Method		*PUBLISH*		
Request-URI		px_PublicUserIdentity		
SIP-Version		*SIP/2.0*		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15] RFC 3903 [60]
route-param	A1	<*sip:*px_pcscf:protected server port of P-CSCF*;lr>,* <*sip:*px_scscf*;lr*>		
route-param	A2	<*sip:*px_pcscf: unprotected server port of P-CSCF (optional)*;lr>, <sip:*px_scscf*;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		px_PublicUserIdentity		
tag		must be present, value not checked but stored for later reference		
To				RFC 3261 [15]
addr-spec		px_PublicUserIdentity		
tag		must not be present		
Expires		**Optional**		RFC 3261 [15]
delta-seconds		same as registration timer		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
Require	A1	**Optional**		RFC 3261 [15] RFC 3329 [21]
option-tag		*Not checked*		
Proxy-Require	A1	**Optional**		RFC 3261 [15] RFC 3329 [21]
option-tag		*Not checked*		
CSeq				RFC 3261 [15]
value		must be present, value not checked		
method		*PUBLISH*		
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	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Event				RFC 3265 [34] RFC 3680 [22] RFC 3903 [60]
event-type		*value not checked*		
SIP-ETag		optional		RFC 3903 [60]
entry-tag				
Content-Length				RFC 3261 [15]
value		length of request body, if such is present		
Message-body		optional		

Condition	Explanation

A1	IMS security (A.6a/2)
A2	early IMS security (A.6a/1)

Note1: All choices for applicable conditions are described for each header.

A.4.4 200 OK for PUBLISH

Header/param	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	px_PublicUserIdentity		
tag	px_ToTagSubscribeDialog		
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:*px_scscf>		
Expires			RFC 3261 [15] RFC 3903 [60]
delta-seconds	600000		
SIP-ETag			RFC 3903 [60]
entry-tag	unique generated tag for every request		
Content-Length			RFC 3261 [15]
value	0		

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 Cleint

*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 Cleint
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-len - DUID	OPTION_CLIENTID (1) Length of the DUID of Client Set to DUID of Client
option-code - option-len - requested-option-code	OPTION_ORO (6) Check Specific message contents in test case 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-len - DUID	OPTION_CLIENTID (1) Length of the DUID of client Set to DUID of Client
option-code - option-len - DUID	OPTION_SERVERID (21) Length of the DUID of Server 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.

C.1 Introduction

This annex specifies the general test procedure required to get the UE to activate PDP context, discover P-CSCF and register to IMS services. Since 3GPP TS 24.229[10] specifies two options for both PDP context activation and P-CSCF discovery, the UE specific general test procedure depends on the option selected by the UE. The generic registration procedure has also been specified for two cases: for UE supporting full IMS security according to [14] TS 33.203 then the generic registration procedure in , see section C2 is run; and for UE supporting early IMS security according to [59] TR 33.978 then the generic registration procedure in , see section C2a is run.

Section C.5 defines a procedure to handle PUBLISH requests that may be send from UEs with IMS applications e.g. OMA PoC.

C.2 Generic Registration Test Procedure – IMS support

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]).

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	→		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.
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: The default message contents in annex A are used.

C.2a Generic Registration Test Procedure – early IMS security

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]).

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 of early IMS security. SS waits for the UE to send an initial REGISTER request.

7 The SS responds to the REGISTER request with valid 200 OK response,

8 The SS waits for the UE to send a SUBSCRIBE request.

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	→		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	Including allocated IP address. 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.
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 early IMS security 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: The default message contents in annex A are used.

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 occure at any time after a successful IMS registration.

The generic test procedure:

1 SS receives from the UE a PUBLISH request.

2 The SS responds to the PUBLISH request with a valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		PUBLISH	The UE sends a PUBLISH request (A.4.3).
2	←		200 OK	The SS responds with 200 OK (A.4.4).

NOTE: The default message contents in annex A are used.

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_HomeDomainName	3gpp.org	
px_PublicUserIdentity	sip:localuser@3gpp.org	
px_PrivateUserIdentity	privateuser@3gpp.org	
IMS registration parameters derived from IMSI when using USIM application		TS 23.003 [32]
px_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	
CSCF domain names		
px_pcscf	pcscf.3gpp.org	(FQDN that resolves to the IP address of SS)
px_scscf	scscf.3gpp.org	(FQDN that does not resolve to the IP address of SS)

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 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.

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 is 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)

The programming of this EF is a test house option.

E.3.2.2 EF$_{DOMAIN}$ (Home Network Domain Name)

The programming of this EF is a test house option.

E.3.2.3 EF$_{IMPU}$ (IMS public user identity)

The programming of this EF is a test house option.

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 [34.108].

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)

The programming of this EF is a test house option.

E.3.2.7 EF$_{P\text{-}CSCF}$ (P-CSCF Address)

This EF does not apply for 3GPP and shall not be used by a terminal using a 3GPP access network or a 3GPP Interworking WLAN.

The programming of this EF is a test house option.

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.

Annex F (informative): Change history

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version - Current	Version -New	Doc-2nd-Level

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	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
				update				
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	70	-	Clarify parameter description in specific message contets	F	6.2.0	6.3.0	R5-072111
RP-37	RP-070607	71	-	Update the SDP RFC reference	F	6.2.0	6.3.0	R5-072112
RP-37	RP-070607	72	-	New TC User initiated re-registration for early IMS	F	6.2.0	6.3.0	R5-072113
RP-37	RP-070607	73	-	Correction to IMS CC test case 12.4	F	6.2.0	6.3.0	R5-072119
RP-37	RP-070594	74	-	Default message correction for 401 response	F	6.2.0	6.3.0	R5-072504
RP-37	RP-070594	75	-	Correct check of ACK message in 12.9	F	6.2.0	6.3.0	R5-072508
RP-37	RP-070594	76	-	Handling of optional PUBLISH messages	F	6.2.0	6.3.0	R5-072507
RP-37	RP-070607	77	-	Correct the check of SDP answer to the SDP offer	F	6.2.0	6.3.0	R5-072511
RP-37	RP-070607	78	-	Correct the re-invite message in 12.6	F	6.2.0	6.3.0	R5-072481
RP-37	RP-070594	79	-	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	80	-	Format of home domain name within the ISIM	F	6.2.0	6.3.0	R5-072506
RP-37	RP-070607	81	-	New TC Mobile initiated de-registration for early IMS	F	6.2.0	6.3.0	R5-072495

History

Document history		
V6.1.0	March 2007	Publication
V6.2.0	June 2007	Publication
V6.3.0	October 2007	Publication