ETSI TS 136 579-3 V13.2.0 (2022-01)

LTE;
Mission Critical (MC) services over LTE;
Part 3: Mission Critical Push To Talk (MCPTT)
Server Application conformance specification
(3GPP TS 36.579-3 version 13.2.0 Release 13)

Reference
RTS/TSGR-0536579-3vd20

Keywords
LTE

ETSI

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

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

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

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

The present document is part 3 of a multi-part conformance test specification for Mission Critical Push To Talk (MCPTT) over LTE consisting of:

3GPP TS 36.579-1 [2]: "Mission Critical (MC) services over LTE; Part 1: Common test environment"

3GPP TS 36.579-2 [3]: "Mission Critical (MS) services over LTE; Part 2: Mission Critical Push To Talk (MCPTT) User Equipment (UE) Protocol conformance specification"

3GPP TS 36.579-3: "Mission Critical (MC) services over LTE; Part 3: Mission Critical Push To Talk (MCPTT) Server Application conformance specification" (the present specification)

3GPP TS 36.579-4 [4]: "Mission Critical (MC) services over LTE; Part 4: Test Applicability and Implementation Conformance Statement (ICS) proforma specification"

3GPP TS 36.579-5 [5]: "Mission Critical (MC) services over LTE; Part 5: Abstract test suite (ATS)"

1 Scope

The present document specifies the protocol conformance testing for testing a MCPTT Server for compliance to the Mission Critical Push To Talk (MCPTT) over LTE protocol requirements defined by 3GPP. The present document addresses only MCPTT Server-Client, and, MCPTT Server-Server communication scenarios. It does not cover e.g. MCPTT Server-EPS, MCPTT Server-SIP Core, etc. scenarios which involve interfaces which implementation may widely vary.

In particular the present specification contains:

- 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 present document is valid for MCPTT Servers implemented according to 3GPP releases starting from Release 13 up to the Release indicated on the cover page of the present document.

The following information relevant to testing specified in the present document could be found in accompanying specifications:

- default setting of the test parameters TS 36.579-1 [2];
- Implementation Conformance Statement (ICS) TS 36.579-4 [4] and Implementation eXtra Information for Testing (IXIT) TS 36.579-5 [5];
- the applicability of each test case TS 36.579-4 [4].

The present document does not specify the protocol conformance testing for the EPS (LTE) bearers which carry the MCPTT data sent or received by the MCPTT Server. The specification of such testing is out of the scope of RAN5.

2 References

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

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

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

[2] 3GPP TS 36.579-1: "Mission Critical Push To Talk (MCPTT) over LTE protocol conformance testing; Part 1: Common test environment".

[3] 3GPP TS 36.579-2: "Mission Critical Push To Talk (MCPTT) over LTE conformance testing; Part 2: MCPTT Client Application test specification".

[4] 3GPP TS 36.579-4: "Mission Critical Push To Talk (MCPTT) over LTE conformance testing; Part 4: Test Applicability and Implementation Conformance Statement (ICS)".

[5] 3GPP TS 36.579-5: "Mission Critical Push To Talk (MCPTT) over LTE conformance testing; Part 5: Abstract test suite (ATS)".

[6] Void

[7] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT) over LTE; Stage 1".

[8] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services; Stage 2".

[9] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification".

[10] 3GPP TS 24.380: "Mission Critical Push To Talk (MCPTT) floor control; Protocol specification".

[11] 3GPP TS 24.481: "Mission Critical Services (MCS) group management; Protocol specification".

[12] 3GPP TS 24.482: "Mission Critical Services (MCS) identity management; Protocol specification".

[13] 3GPP TS 24.483: "Mission Critical Services (MCS) Management Object (MO)".

[14] 3GPP TS 24.484: "Mission Critical Services (MCS) configuration management; Protocol specification".

[15] 3GPP TS 33.179: "Security of Mission Critical Push-To-Talk (MCPTT)".

[16] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[17] 3GPP TS 24.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 3".

[18] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference Point; Stage 3".

[19] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[20] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[21] 3GPP TS 36.509: "Special conformance testing functions for User Equipment (UE)".

[22] 3GPP TS 36.508: "Common test environments for User Equipment (UE) conformance testing".

[23] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP 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 3GPP TR 21.905 [1].

For the purpose of the present document, the following terms and definitions given in 3GPP TS 24.379 [9] apply:

An MCPTT user is affiliated to an MCPTT group
An MCPTT user is affiliated to an MCPTT group at an MCPTT client
Affiliation status
Group identity
In-progress emergency private call state
In-progress imminent peril group state
MCPTT client ID
MCPTT emergency alert state

MCPTT emergency group state
MCPTT emergency group call state
MCPTT emergency private call state
MCPTT emergency private priority state
MCPTT imminent peril group call state
MCPTT imminent peril group state
MCPTT private emergency alert state
MCPTT speech
Media-floor control entity
Temporary MCPTT group identity
Trusted mutual aid
Untrusted mutual aid

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.179 [7] apply:

In-progress emergency
MCPTT emergency alert
MCPTT emergency group call
MCPTT emergency state
Partner MCPTT system
Primary MCPTT system

For the purpose of the present document, the following terms and definitions given in 3GPP TS 24.380 [10] apply:

MBMS subchannel

For the purpose of the present document, the following terms and definitions given in 3GPP TS 23.179 [8] apply:

Pre-selected MCPTT user profile

3.2 Symbols

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

None

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

ECGI	E-UTRAN Cell Global Identification
FFS	For Further Study
ICS	Implementation Conformance Statement
IPEG	In-Progress Emergency Group
IPEPC	In-Progress Emergency Private Call
IPIG	In-Progress Imminent peril Group
IUT	Implementation Under Test
IXIT	Implementation eXtra Information for Testing
MBMS	Multimedia Broadcast and Multicast Service
MBSFN	Multimedia Broadcast multicast service Single Frequency Network
MCPTT	Mission Critical Push To Talk
MCPTT group ID	MCPTT group IDentity
MEA	MCPTT Emergency Alert
MEG	MCPTT Emergency Group
MEGC	MCPTT Emergency Group Call
MEPC	MCPTT Emergency Private Call
MEPP	MCPTT Emergency Private Priority
MES	MCPTT Emergency State
MIME	Multipurpose Internet Mail Extensions

MIG	MCPTT Imminent peril Group
MIGC	MCPTT Imminent peril Group Call
MONP	MCPTT Off-Network Protocol
MPEA	MCPTT Private Emergency Alert
NAT	Network Address Translation
PLMN	Public Land Mobile Network
QCI	QoS Class Identifier
RTP	Real-time Transport Protocol
SAI	Service Area Identifier
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SS	System Simulator
SSRC	Synchronization SouRCe
TGI	Temporary MCPTT Group Identity
TMGI	Temporary Mobile Group Identity
TP	Transmission Point
	Test Purpose
URI	Uniform Resource Identifier

4 General

4.1 Test methodology

4.1.1 Testing of optional functions and procedures

Any function or procedure which is optional may be subject to a conformance test if it is implemented in the MCPTT Server.

A declaration by the Client supplier (to use the Implementation Conformance Statement (ICS) proforma specified in TS 36.579-4 [4]) is used to determine whether an optional function/procedure has been implemented.

4.1.2 Test interfaces and facilities

Detailed descriptions of the MCPTT Server to MCPTT Client test interfaces and special facilities for testing are provided in 3GPP TS 36.509 [21]. Descriptions of the MCPTT Server to MCPTT Server interface is specified in TS 36.579-1 [2].

4.2 Implicit testing

For some 3GPP MCPTT 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 tests which are not explicitly dedicated to test the feature.

4.3 Repetition of tests

As a general rule, the test cases specified in the present document are highly reproducible and don't need to be repeated unless otherwise stated.

4.4 Handling of differences between conformance requirements in different releases of cores specifications

The conformance requirements which determine the scope of each test case are explicitly copy-pasted from relevant core specifications in the especially dedicated for this section of each test with the title 'Conformance requirements'.

NOTE: When in the copy/pasted text there are references to other specifications the reference numbers will not match the reference numbers used in the present specification. This approach has been taken in order to allow easy copy and then search for conformance requirements in those specifications.

When differences between conformance requirements in different releases of the cores specifications have impact on the Pre-test conditions, Test procedure sequence or/and the Specific message contents, the Conformance requirements related to different releases are specified separately with clear indication of the Release of the spec from which they were copied.

When there is no Release indicated for a conformance requirement text, this should be understood either as the Conformance requirements in the latest version of the spec with release = the TC Applicability release (which can be found in TS 36.579-4 [4], Table 4-2: Applicability of tests and additional information for testing, column 'Release'), or, as the Conformance requirements in the latest version of the spec of the release when the feature was introduced to the core specs.

4.5 Reference conditions

The reference environments used by all signalling and protocol tests are specified in TS 36.579-1 [2]. Where a test requires an environment that is different, this will be specified in the test itself.

4.6 Generic setup procedures

A set of basic generic procedures for MCPTT Client-Server and MCPTT Client-Client communication are described in TS 36.579-1 [2]. These procedures will be used in numerous test cases throughout the present document.

5 MCPTT Client Configuration

5.1 MCPTT Server - MCPTT Client / Configuration / Authentication / User Authorisation / UE Configuration / User Profile

5.1.1 Test Purpose (TP)

(1)

```
with { IUT (MCPTT Server) connected to PLMN1 }
ensure that {
  when { the SS-UE1 (MCPTT client) activates an MCPTT application and requests MCPTT initialisation
}
    then { IUT (MCPTT Server) provides the initial UE configuration and performs MCPTT User
Authentication and provides id_token, access_token and refresh token to the successfully
authenticated user}
            }
```

(2)

```
with { IUT (MCPTT Server) having authenticated the SS-UE1 (MCPTT client) }
ensure that {
  when { the SS (MCPTT Client) initiates key management authorization }
    then { IUT (MCPTT Server) provides identity management key material }
            }
```

(3)

```
with { IUT (MCPTT Server) having provided identity management key material }
ensure that {
  when { the SS-UE1 (MCPTT client) requests user service authorization }
    then { IUT (MCPTT Server) responds to the SS (MCPTT Client) with SIP 200 (OK) messages }
            }
```

(4)

```
with { IUT (MCPTT Server) having provided service authorization }
ensure that {
  when { the SS-UE1 (MCPTT client) requests configuration management authorization}
    then { IUT (MCPTT Server) responds to the SIP SUBSCRIBE message with a SIP 200 (OK) message and
sends a SIP NOTIFY message containing the XCAP-URI of the documents and sends the MCPTT UE
Configuration Document and MCPTT User Profile Configuration Document MCPTT Service Configuration
Document via HTPP 200 (OK) messages in response to HTTP GET requests }
            }
```

(5)

```
with { IUT (MCPTT Server) having provided user configuration data }
ensure that {
  when { the SS-UE1 (MCPTT client) requests group management authorization }
    then { IUT (MCPTT Server) responds to the SS (MCPTT Client) with SIP 200 (OK) messages and sends
the XCAP-URI of the Group documents via a SIP NOTIFY message and sends the Group Document 'MCPTT UE
Configuration document' via a HTPP 200 (OK) message in response to a HTTP GET request and sends the
group key transport payloads (GKTP) document via a SIP NOTIFY message }
            }
```

(6)

```
with { IUT (MCPTT Server) having provided all required configuration data }
ensure that {
  when { the SS-UE1 (MCPTT client) requests to refresh its service settings }
    then { IUT (MCPTT Server) responds to the SS (MCPTT Client) with a SIP 200 (OK) message }
            }
```

5.1.2 Conformance requirements

References: The conformance requirements covered in the present TC are specified in: TS 24.482 clause 6.3.1, Annex A.2.1.3, Annex A.2.3, TS 24.484 clauses 4.3, 4.4, 6.2.3, 6.3.1.2, 6.3.2.3, 6.3.13.3.2.2, TS 24.481 clauses 6.2.4, 6.3.3.3, 6.3.13.3.2.2, TS 24.379 clauses 7.3.2, 7.3.3, 7.3.4, TS 33.179 clauses 5.6.1, 7.2.3, Annex D.1. Unless otherwise stated these are Rel-13 requirements.

[TS 24.482, clause 6.3.1]

Upon receipt of an OIDC Authentication Request message as specified in the OpenID Connect 1.0 [6] and IETF RFC 6749 [5] via a secure TLS tunnel between the identity management client and the authorisation endpoint of the IdM server, the IdM server:

1) shall validate the received OIDC Authentication Request message as specified in the OpenID Connect 1.0 [6] and IETF RFC 6749 [5];

2) shall generate an HTTP 200 (OK) response according to IETF RFC 2616 [4] including form data to prompt the MCPTT user for their username and password credentials; and

NOTE 1: The username will be the MCPTT user's MC ID.

3) shall send the HTTP 200 (OK) response towards the IdM client.

Upon receipt of an HTTP POST request method from the IdM client containing the MCPTT user's username and password, the IdM server authenticates the MCPTT user and:

NOTE 2: Other methods of authentication can be used by the MCPTT service provider and are not defined by the OIDC specifications. 3GPP TS 33.179 [2] has defined username and password as a mandatory authentication method to be supported for MCPTT, hence a procedure to realize that method is included here.

1) shall generate an OIDC Authentication Response message as specified in OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

   a) shall generate an HTTP 302 (FOUND) response according to IETF RFC 2616 [4]; and

b) shall include the required parameters including the authorization_code as specified in 3GPP TS 33.179 [2] in the query component of the redirection URI contained in the Location header field of the HTTP FOUND request method using the "application/x-www-form-urlencoded" format as specified in W3C.REC-html401-19991224 [7]; and

2) shall send the HTTP 302 (FOUND) response towards the IdM client.

Upon receipt of an OIDC Token Request message via a secure TLS tunnel established between the identity management client and the token endpoint of the IdM server, the IdM server:

1) shall validate the OIDC Token Request message and if valid shall generate an OIDC Token Response message as specified in OpenID Connect 1.0 [6] and IETF RFC 6749 [5] with the following clarifications:

   a) shall generate an HTTP 200 (OK) response according to IETF RFC 2616 [4];

   b) shall based on the received MC ID obtained from the received user authentication credentials, determine the MCPTT ID of the MCPTT user;

   c) shall include an id_token, access_token and refresh_token and MCPTT ID as specified in 3GPP TS 33.179 [2]; and

   d) shall include the other required parameters as specified in OpenID Connect 1.0 [6] and IETF RFC 6749 [5]; and

2) shall send the HTTP 200 (OK) response towards the IdM client.

[TS 24.482, Annex A.2.1.3]

The HTTP client in the network entity is configured with the following parameters:

1) a home HTTP proxy FQDN; and

2) a home HTTP proxy port.

The HTTP client in the network entity shall send and receive all HTTP messages via the home HTTP proxy.

The HTTP client in the network entity shall insert an X-3GPP-Asserted-Identity header field as specified in 3GPP TS 24.109 [15] in the HTTP request and shall set X-3GPP-Asserted-Identity header field to the identity of the HTTP client in the network entity. The identity of the HTTP client in the network entity can be a public service identity, an MCPTT group ID, or an MCPTT ID.

[TS 24.482, Annex A.2.3]

The HTTP server shall support the server role of IETF RFC 2616 [4].

Upon reception of an HTTP request:

1) if the received HTTP request does not contain an Authorization header field with the "Bearer" authentication scheme and a bearer access token as specified in IETF RFC 6750 [14] and the received HTTP request does not contain an X-3GPP-Asserted-Identity header field as specified in 3GPP TS 24.109 [15], the HTTP server shall reject the request with HTTP 403 (Forbidden) response;

2) if the received HTTP request contains an Authorization header field with the "Bearer" authentication scheme and a bearer access token as specified in IETF RFC 6750 [14];

   a) the HTTP server shall validate the bearer access token as specified in IETF RFC 6750 [14]; and

   b) the HTTP server shall consider the MCPTT ID derived from the bearer access token as the identity of the sender of the HTTP request; and

3) if the received HTTP request does not contain an Authorization header field with the "Bearer" authentication scheme and a bearer access token as specified in IETF RFC 6750 [14] and the received HTTP request contains an X-3GPP-Asserted-Identity header field as specified in 3GPP TS 24.109 [15], the HTTP server shall consider the URI in the X-3GPP-Asserted-Identity header field as the identity of the sender of the HTTP request.

[TS 24.484, clause 4.3]

The MCPTT server obtains the MCPTT service configuration document that contains the mission critical organisation configured parameters that defined the behaviour of the MCPTT service from the configuration management server.

The format of the MCPTT service configuration document downloaded to the MCPTT server is defined in subclause 7.5.

The MCPTT server obtains the MCPTT service configuration document that contains the mission critical organisation configured parameters that defined the behaviour of the MCPTT service from the configuration management server.

The MCPTT server subscribes to the MCPTT service configuration document for each mission critical organisation that is provisioned that is supported by the MCPTT server using the procedure specified in subclause 6.3.13.2.3. How the MCPTT server is provisioned with the identities of the mission critical organisations is out of scope of the present document.

If the MCPTT service configuration document has been updated since the current version stored at the MCPTT server, then the MCPTT server will receive a SIP NOTIFY request containing an HTTPS URI of the MCPTT service configuration document. Retrieval by the MCPTT server, using the notified HTTPS URI, of the MCPTT service configuration document is performed as specified in subclause 6.3.3.2.3.

NOTE: The MCPTT server can be notified of changes to the MCPTT service management configuration document at any time while operating the MCPTT service.

The format of the MCPTT service configuration document downloaded to the MCPTT server is defined in subclause 7.5.

[TS 24.484, clause 4.4]

The following applies to the configuration management server used for online configuration.

The configuration management server needs to convert the MCPTT UE initial configuration document received from a MCPTT administrator into an appropriate format for configuration of the MCPTT UE initial configuration MO.

If the MCPTT UE initial configuration MO contains a <default-user-profile> element that identifies a MCPTT user profile configuration document, the configuration management server needs to convert the identified MCPTT user profile configuration document received from a MCPTT administrator into an appropriate format for configuration of the MCPTT user profile configuration MO.

Once an MCPTT User Profile configuration document has been created or updated by the MCPTT UE, the configuration management server uses the procedures specified in 3GPP TS 29.283 [7] to store MCPTT user profile configuration document as the user profile in the MCPTT user database.

In order to download MCPTT the user profile configuration document to an MCPTT UE or to support an MCPTT UE updating the MCPTT user profile configuration document, the configuration management server uses the procedures specified in 3GPP TS 29.283 [7] to obtain the MCPTT user profile from the MCPTT user database.

In order to be notified of changes to an MCPTT user profile configuration document that have been subscribed to by an MCPTT UE, the configuration management server uses the procedures specified in 3GPP TS 29.283 [7] to be notified of changes to the MCPTT user profile stored in the MCPTT user database.

In order to delete the MCPTT user profile when requested by an MCPTT UE, the configuration management server uses the procedures specified in 3GPP TS 29.283 [7] to delete the MCPTT user profile from the MCPTT user database.

NOTE: The configuration management server and group management server functionality for offline configuration is out of scope of the present document.

[TS 24.484, clause 6.2.3]

The MCPTT server shall send the HTTP request as specified for the HTTP client in the network entity in annex A of 3GPP TS 24.382 [6].

[TS 24.484, clause 6.2.4]

The CMS shall handle the HTTP request as specified for the HTTP server in annex A of 3GPP TS 24.382 [6].

The CMS shall be configured with an authorized MCPTT server list, containing public service identities of MCPTT servers of the MCPTT provider of the CMS.

When handling an HTTP request, the CMS shall determine the identity of the sender of the HTTP request as specified in 3GPP TS 24.382 [6], and shall use the identity of the sender of the HTTP request as an authenticated identity when performing the authorization.

[TS 24.484, clause 6.3.1.2]

A CMS shall support subclause 6.2.1 "*Document Management*", and subclause 6.2.4 "*Access Permissions*" of OMA OMA-TS-XDM_Core-V2_1 [2] and subclause 6.3.13.3 for accepting subscriptions to configuration management documents.

[TS 24.484, clause 6.3.2.3]

A CMS shall support receiving XML documents of the application usages specified in subclause 7.2.1, subclause 7.3.1, subclause 7.4.1 and subclause 7.5.1according to procedures specified in IETF RFC 4825 [14] "*PUT Handling*" where the Request-URI of the HTTP PUT request identifies an XML document and include the "auid" as per the appropriate application usage in clause 7.

[TS 24.484, clause 6.3.13.3.2.2]

Upon reception of an initial SIP SUBSCRIBE request:

a) with the Event header field set to xcap-diff;

b) with the Request-URI set to own public service identity for performing subscription proxy function of the CMS;

c) with a P-Asserted-Identity header field not containing an identity listed in the authorized MCPTT server list specified in subclause 6.2.4;

d) with an application/vnd.3gpp.mcptt-info+xml MIME body containing the <mcptt-access-token> element;

e) with an application/resource-lists+xml MIME body; and

f) with the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24 229 [12]), in a P-Asserted-Service header field according to IETF RFC 6050 [23];

the CMS:

a) if an <EncryptedData> XML tag is included in the application/vnd.3gpp.mcptt-info+xml MIME body and the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/vnd.3gpp.mcptt-info+xml MIME body;

b) if an <EncryptedData> XML tag is included in the application/resource-lists+xml MIME body and the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/resource-lists+xml MIME body;

c) shall identify the originating MCPTT ID from <mcptt-access-token> element received in the application/vnd.3gpp.mcpttinfo+xml MIME body and shall use the originating MCPTT ID as an authenticated identity when performing the authorization;

d) if the authenticated identity is not authorized to subscribe to notification of changes of any resource in the application/resource-lists+xml MIME body, shall reject the request with a SIP 403 (Forbidden) response and shall not continue with rest of the steps;

e) act as a notifier according to IETF RFC 5875 [11]. Additionally, if an XCAP URI in the "uri" attribute of the <entry> element of the application/resource-lists+xml MIME body of the initial SIP SUBSCRIBE request contains an "auid" parameter set to an application usage identifying a configuration management document as described in clause 7;

shall return the XCAP URI identifying the configuration management document in SIP NOTIFY requests associated with a subscription created as result of the received initial SIP SUBSCRIBE request.

Upon sending a SIP NOTIFY request associated with a subscription created as result of the received initial SIP SUBSCRIBE request, if the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, the CMS shall perform the confidentiality protection procedures and integrity protection procedures defined in 3GPP TS 24.379 [9] for MCPTT server.

Upon reception of a SIP re-SUBSCRIBE request:

a) with the Event header field set to xcap-diff; and

b) with an application/resource-lists+xml MIME body;

the CMS:

a) if an <EncryptedData> XML tag is included in the application/resource-lists+xml MIME body of the received SIP re-SUBSCRIBE request and the CSK was received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/resource-lists+xml MIME body; and

b) act as a notifier according to IETF RFC 5875 [11]. Additionally, if an XCAP URI in the "uri" attribute of the <entry> element of the application/resource-lists+xml MIME body of the SIP re-SUBSCRIBE request contains an "auid" parameter set to an application usage identifying a configuration management document as described in clause 7:

and for which there is no related subscription established according to the subclause 6.3.13.3.2.3, shall return the XCAP URI identifying the configuration management document in SIP NOTIFY requests associated with a subscription created as result of the received initial SIP SUBSCRIBE request.

[TS 24.481, clause 6.2.4]

The MCPTT server shall send the HTTP request as specified for the HTTP client in the network entity in annex A of 3GPP TS 24.382 [10].

The MCPTT server shall perform the procedures in subclause 6.2.2 specified for GC.

[TS 24.481, clause 6.3.3.3]

A GMS shall support handling an HTTP GET request from a GMC according to procedures specified in IETF RFC 4825 [22] "*GET Handling*" where the Request-URI of the HTTP GET request identifies an XML document of the application usage specified in subclause 7.2.

[TS 24.481, clause 6.3.13.3.2.2]

Upon reception of an initial SIP SUBSCRIBE request:

a) with the Event header field set to xcap-diff;

b) with the Request-URI set to own public service identity for performing subscription proxy function of the GMS;

c) with a P-Asserted-Identity header field not containing an identity listed in the authorized MCPTT server list specified in subclause 6.2.5.1 and not containing an identity listed in the authorized GMS list as specified in subclause 6.2.5.1;

d) with an application/vnd.3gpp.mcptt-info+xml MIME body containing the <mcptt-access-token> element;

e) with an application/resource-lists+xml MIME body; and

f) with the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24 229 [12]), in a P-Asserted-Service header field according to IETF RFC 6050 [14];

the GMS:

a) if an <EncryptedData> XML tag is included in the application/vnd.3gpp.mcptt-info+xml MIME body and the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/vnd.3gpp.mcptt-info+xml MIME body;

b) if an <EncryptedData> XML tag is included in the application/resource-lists+xml MIME body and the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/resource-lists+xml MIME body;

c) shall identify the originating MCPTT ID from <mcptt-access-token> element received in the application/vnd.3gpp.mcptt-info+xml MIME body and shall use the originating MCPTT ID as an authenticated identity when performing the authorization;

d) if the authenticated identity is not authorized to subscribe to notification of changes of any resource in the application/resource-lists+xml MIME body, shall reject the request with a SIP 403 (Forbidden) response and shall not continue with rest of the steps;

e) act as a notifier according to IETF RFC 5875 [13]. Additionally, if an XCAP URI in the "uri" attribute of the <entry> element of the application/resource-lists+xml MIME body of the initial SIP SUBSCRIBE request identifies:

1) a group document addressed by a group ID as described in subclause 7.2.10.2 where the group ID is an MCPTT group ID owned by an MCPTT provider other than the MCPTT provider of the GMS; or

2) a element of an MCPTT GKTP document as described in subclause 7.7.10 where the group ID is an MCPTT group ID owned by an MCPTT provider other than the MCPTT provider of GMS;

shall perform the procedure in subclause 6.3.13.3.2.4 for each such MCPTT group ID and shall interwork information of received SIP NOTIFY requests in subclause 6.3.13.3.2.4 in SIP NOTIFY requests associated with a subscription created as result of the received initial SIP SUBSCRIBE request.

Upon sending a SIP NOTIFY request associated with a subscription created as result of the received initial SIP SUBSCRIBE request, if the CSK is received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, the GMS shall perform the confidentiality protection procedures and integrity protection procedures defined in 3GPP TS 24.379 [5] for MCPTT server.

Upon reception of a SIP re-SUBSCRIBE request:

a) with the Event header field set to xcap-diff; and

b) with an application/resource-lists+xml MIME body;

the GMS:

a) if an <EncryptedData> XML tag is included in the application/resource-lists+xml MIME body of the received SIP re-SUBSCRIBE request and the CSK was received in an application/mikey MIME body of the initial SIP SUBSCRIBE request, shall decrypt the application/resource-lists+xml MIME body; and

b) act as a notifier according to IETF RFC 5875 [13]. Additionally, if an XCAP URI in the "uri" attribute of the <entry> element of the application/resource-lists+xml MIME body of the SIP re-SUBSCRIBE request identifies:

1) a group document addressed by a group ID as described in subclause 7.2.10.2 where the group ID is an MCPTT group ID owned by an MCPTT provider other than the MCPTT provider of the GMS; or

2) a element of an MCPTT GKTP document as described in subclause 7.7.10 where the group ID is an MCPTT group ID owned by an MCPTT provider other than the MCPTT provider of GMS;

and for which there is no related subscription established according to the subclause 6.3.13.3.2.4, shall perform the procedure in subclause 6.3.13.3.2.4 for each such MCPTT group ID and shall interwork information of received SIP NOTIFY requests in subclause 6.3.13.3.2.4 in SIP NOTIFY requests associated with a subscription created as result of the received initial SIP SUBSCRIBE request.

[TS 24.379, clause 7.3.2]

The MCPTT server shall support obtaining service authorization specific information from the SIP REGISTER request sent from the MCPTT client and included in the body of a third-party SIP REGISTER request.

NOTE 1: 3GPP TS 24.229 [4] defines how based on initial filter criteria the SIP REGISTER request sent from the UE is included in the body of the third-party SIP REGISTER request.

Upon receiving a third party SIP REGISTER request with a message/sip MIME body containing the SIP REGISTER request sent from the MCPTT client containing an application/vnd.3gpp.mcptt-info+xml MIME body with an <mcptt-access-token> element and an <mcptt-client-id> element within a message/sip MIME body of the SIP REGISTER request sent from the MCPTT client, the MCPTT server:

1) shall identify the IMS public user identity from the third-party SIP REGISTER request;

2) shall identify the MCPTT ID from the SIP REGISTER request sent from the MCPTT client and included in the message/sip MIME body of the third-party SIP REGISTER request by following the procedures in subclause 7.3.1A;

3) shall perform service authorization for the identified MCPTT ID as described in 3GPP TS 33.179 [46];

4) if service authorization was successful, shall bind the MCPTT ID to the IMS public user identity; and

NOTE 2: The MCPTT server will store the binding MCPTT ID, IMS public user identity and an identifier addressing the MCPTT server in an external database.

5) if a Resource-Share header field with the value "supported" is contained in the "message/sip" MIME body of the third-party REGISTER request, shall bind the MCPTT ID to the identity of the MCPTT UE contained in the "+g.3gpp.registration-token" header field parameter in the Contact header field of the incoming third-party REGISTER request.

[TS 24.379, clause 7.3.3]

The MCPTT server shall support obtaining service authorization specific information from a SIP PUBLISH request for MCPTT server settings.

Upon receiving a SIP PUBLISH request containing:

1) an Event header field set to the "poc-settings" value;

2) an application/poc-settings+xml MIME body; and

3) an application/vnd.3gpp.mcptt-info+xml MIME body containing an <mcptt-access-token> element and an <mcptt-client-id> element;

the MCPTT server:

1) shall identify the IMS public user identity from the P-Asserted-Identity header field;

2) shall perform the procedures in subclause 7.3.1A;

3) if the procedures in subclause 7.3.1A were not successful shall send a SIP 403 (Forbidden) response towards the MCPTT server with the warning text set to: "140 unable to decrypt XML content " in a Warning header field as specified in subclause 4.4, and not continue with the rest of the steps in this subclause;

4) shall perform service authorization for the identified MCPTT ID as described in 3GPP TS 33.179 [46];

5) if service authorization was successful:

   a) shall bind the MCPTT ID to the IMS public user identity;

   b) if a Resource-Share header field with the value "supported" was included in the "message/sip" MIME body of the third-party REGISTER request, shall bind the MCPTT ID to the identity of the MCPTT UE contained in the "+g.3gpp.registration-token" header field parameter in the Contact header field of the third-party REGISTER request that contained this IMS public user identity;

NOTE 1: The MCPTT server will store the binding MCPTT ID, IMS public user identity and an identifier addressing the MCPTT server in an external database.

   c) shall download the MCPTT user profile from the MCPTT user database as defined in 3GPP TS 29.283 [73] if not already stored at the MCPTT server;

   d) if multiple MCPTT user profiles are stored at the MCPTT server or downloaded for the MCPTT user from the MCPTT user database, shall determine the pre-selected MCPTT user profile by identifying the MCPTT user profile (see the MCPTT user profile document in 3GPP TS 24.384 [50]) in the collection of MCPTT user profiles that contains a <Pre-selected-indication> element; and

NOTE 2: If only one MCPTT user profile is stored at the MCPTT server or only one MCPTT user profile is downloaded from the MCPTT user database, then by default this MCPTT user profile is the pre-selected MCPTT user profile.

e) if an <ImplicitAffiliations> element is contained in the <OnNetwork> element of the MCPTT user profile document with one or more <entry> elements containing an MCPTT group ID (see the MCPTT user profile document in 3GPP TS 24.384 [50]) for the served MCPTT ID, shall perform implicit affiliation as specified in subclause 9.2.2.2.15;

6) if service authorization was not successful, shall send a SIP 403 (Forbidden) response towards the MCPTT server with the warning text set to: "101 service authorisation failed" in a Warning header field as specified in subclause 4.4, and not continue with the rest of the steps in this subclause;

7) shall process the SIP PUBLISH request according to rules and procedures of IETF RFC 3903 [37] and if processing of the SIP request was not successful, do not continue with the rest of the steps;

8) shall cache the received MCPTT service settings until the MCPTT service settings expiration timer expires;

9) shall send a SIP 200 (OK) response according 3GPP TS 24.229 [4]; and

10) shall use the Answer-Mode Indication setting in the <am-settings> element of the poc-settings event package as the current Answer-Mode Indication of the MCPTT client.

[TS 24.379, clause 7.3.4]

Upon receiving a SIP PUBLISH request containing:

1) an Event header field set to the "poc-settings" value;

2) an application/poc-settings+xml MIME body; and

3) an application/vnd.3gpp.mcptt-info+xml MIME body containing an <mcptt-request-uri> element and an <mcptt-client-id> element;

The MCPTT server:

1) shall identify the IMS public user identity from the P-Asserted-Identity header field;

2) shall perform the procedures in subclause 7.3.1A;

3) if the procedures in subclause 7.3.1A were not successful, shall send a SIP 403 (Forbidden) response towards the MCPTT server with the warning text set to: "140 unable to decrypt XML content" in a Warning header field as specified in subclause 4.4, and not continue with the rest of the steps in this subclause;

4) shall verify that a binding between the IMS public user identity in the Request-URI and the MCPTT ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml exists at the MCPTT server;

5) if a binding exists between the IMS public user identity and the MCPTT ID in the request and the validity period of the binding has not expired:

   a) shall download the MCPTT user profile from the MCPTT user database as defined in 3GPP TS 29.283 [73] if not already stored at the MCPTT server;

   b) if multiple MCPTT user profiles are stored at the MCPTT server or downloaded for the MCPTT user from the MCPTT user database, shall determine the pre-selected MCPTT user profile by identifying the MCPTT user profile (see the MCPTT user profile document in 3GPP TS 24.384 [50]) in the collection of MCPTT user profiles that contains a <Pre-selected-indication> element; and

   NOTE: If only one MCPTT user profile is stored at the MCPTT server or only one MCPTT user profile is downloaded from the MCPTT user database, then by default this MCPTT user profile is the pre-selected MCPTT user profile.

   c) if an <ImplicitAffiliations> element is contained in the <OnNetwork> element of the MCPTT user profile document with one or more <entry> elements containing an MCPTT group ID (see the MCPTT user profile document in 3GPP TS 24.384 [50]) for the served MCPTT ID, shall perform implicit affiliation as specified in subclause 9.2.2.2.15.

6) if a binding does not exist between the IMS public user identity and the MCPTT ID in the request or the binding exists, but the validity period of the binding has expired, shall reject the SIP PUBLISH request with a SIP 404 (Not Found) response and not continue with any of the remaining steps;

7) shall process the SIP PUBLISH request according to rules and procedures of IETF RFC 3903 [37] and if processing of the SIP request was not successful, do not continue with the rest of the steps;

8) shall cache the received MCPTT service settings until the MCPTT service settings expiration timer expires;

9) shall send a SIP 200 (OK) response according 3GPP TS 24.229 [4]; and

10) shall use the Answer-Mode Indication setting in the <am-settings> element of the poc-settings event package as the current Answer-Mode Indication of the MCPTT client.

[TS 33.179 clause 5.6.1]

For key management authorization, the KM client in the UE presents an access token to the KMS over HTTP. The KMS validates the access token and if successful, provides user specific key material back to the UE KM client based on the MCPTT ID of the user. This includes identity based key information used for media and signalling protection.

For user service authorization, the MCPTT client in the UE presents an access token to the MCPTT server over SIP. The MCPTT server validates the access token and if successful, authorizes the user for full MCPTT services and sends an acknowledgement back to the MCPTT client. The MCPTT server then maps and maintains the IMPU to MCPTT ID association. The MCPTT ID to IMPU association shall only be known to the application layer. The SIP message used to convey the access token from the MCPTT client to the MCPTT server may be either a SIP REGISTER or SIP PUBLISH message.

The UE can now perform configuration management authorization and download the user profile. Following the flow described in subclause 10.1.4.2 of 3GPP TS 23.179 [2] "MCPTT user obtains the user profile (UE initiated)", the Configuration Management (CM) client in the UE sends an access token in the user profile query to the Configuration Management server over HTTP. The CM server receives the request and validates the access token, and if valid, the CM server uses the MCPTT ID to obtain the user profile from the MCPTT user database. The CM server then sends the user profile back to the CM client over HTTP.

Upon receiving the user's profile, the Group Management (GM) client in the UE can now perform group management authorization. The GM client obtains the user's group membership information from the user's profile, and following the flow shown in clause 10.1.5.2 of 3GPP TS 23.179 [2] "Retrieve group configurations at the group management client", the Group Management (GM) client in the UE sends an access token in the Get group configuration request to the host GM server of the group membership over HTTP. The GM server validates the access token, and if valid, completes the flow. As part of group management authorization, group key information is provided as per subclause 7.3.2 of the present document.

[TS 33.179 clause 7.2.3]

The procedure for the provision of identity-specific key material when the MCPTT proxy is supported between the KMS and the KMS client is described in figure 7.2.3-1. The procedure is the same whether the key management client in the MCPTT UE, MCPTT Server or group management server is making the request.

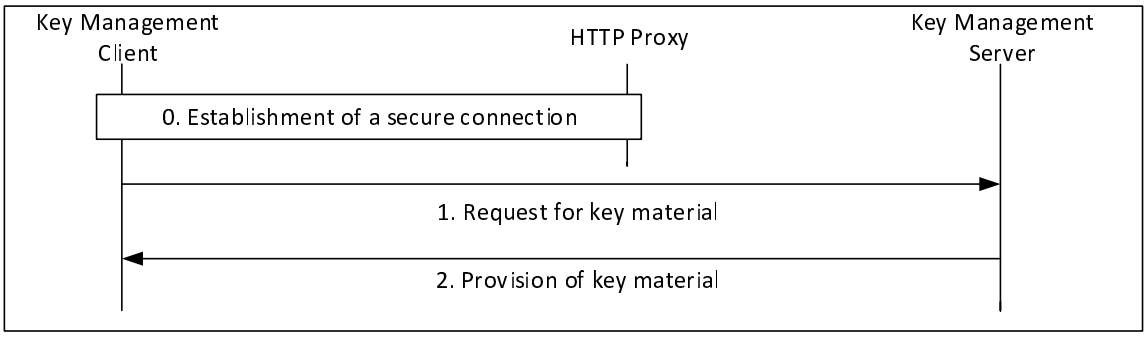

Figure 7.2.3-1: Provisioning of key material via the HTTP proxy

The procedure in figure 7.2.3-1 is now described step-by-step.

0) The key management client establishes a connection to the MCPTT KMS. As with other elements in the Common Services Core, the connection routed via, and secured by, the HTTP Proxy. The message flow below is within this secure connection.

NOTE: Additionally, the connection between the MCPTT KMS and the HTTP Proxy is secured according to clause 8.

1) The key management client makes a request for user key material from the MCPTT KMS. The request contains details of the identity (e.g. the MCPTT ID) requested for key management, and the time for which the key material is required.

2) The KMS provides a response containing key material. The response includes the type of key material, the period of use for the material and any domain-specific parameters required for its use. For public safety use, the key material itself shall be wrapped using a 256-bit transport key (TrK). The TrK is distributed via an out-of-band mechanism along with a 32-bit identifier, TrK-ID.

The procedure for the provisioning of identity-specific key material when the MCPTT proxy is not used between the KMS and the KMS client is as described in Figure 7.2.3-2.

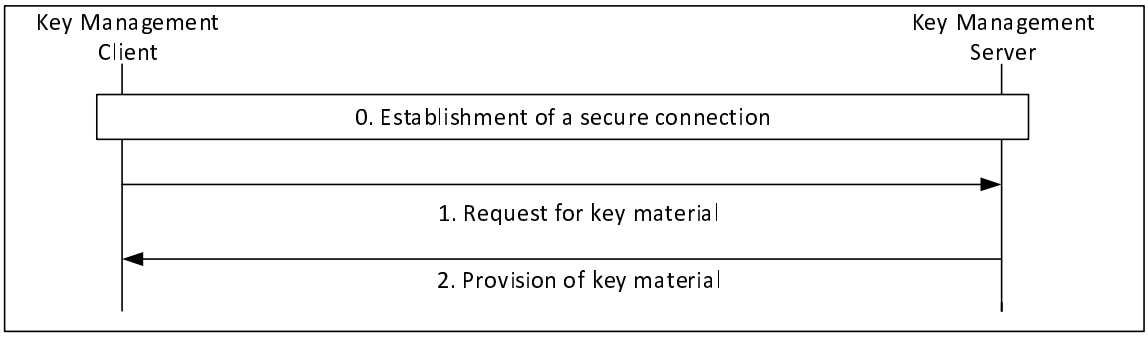

Figure 7.2.3-2: Provisioning of key material without a proxy

The procedure in Figure 7.2.3-2 is now described step-by-step:

0) The key management client establishes a direct HTTPS connection to the MCPTT KMS. The following message flow is within this secure connection.

1) The key management client makes a request for user key material from the MCPTT KMS. The request contains details of the identity requested for key management, and the time at which the key material is required.

2) The KMS provides a response containing key material. The response includes the type of key material, the period of use for the material and any domain-specific parameters required for its use. Optionally, the key material itself may also be wrapped using a 256-bit transport key (TrK), distributed via an out-of-band mechanism along with a 32-bit identifier (TrK-ID).

As a result of this procedure, the key management client has securely obtained key material for use within the MCPTT system.

[TS 33.179 Annex D.1]

All KMS communications are made via HTTPS. The MCPTT key management client is provisioned via XML content in the KMS's response. The XML content is designed to be extendable to allow KMS/client providers to add further information in the XML. Where the interface is extended, a different XML namespace should be used (so that may be ignored by non-compatible clients).

It is assumed that transmissions between the KMS and the key management client are secure and that the KMS has authenticated the identity of the key management client.

Additionally, to allow the transmission of key material securely between a secure element within the KMS and a secure element within the key management client, a security extension is defined which allows messages to be signed and key material to be encrypted using a shared Transport Key (TrK).

5.1.3 Test description

5.1.3.1 Pre-test conditions

System Simulator:

- SS-UE1 (MCPTT client)
- For the underlying "transport bearer" over which the SS-UE1 (MCPTT client) and the MCPTT Server will communicate Parameters are set to the default parameters for the basic E-UTRA Single cell network scenarios, as defined in 3GPP TS 36.508 [22] clause 4.4. The simulated Cell 1 shall belong to PLMN1 (the PLMN specified for MCPTT operation in the MCPTT configuration document).

IUT:

- IUT (MCPTT Server)
- The IUT (MCPTT Server) consists of all sub-systems of the Common Services Core, including the Group Management Server, the Configuration Management Server, the Key Management Server, the Identity Management Server, the HTTP Server, and the SIP AS. The IUT (MCPTT Server) also consists of all sub-systems of the MCPTT Server, including the Media Distribution Function, the MCPTT User Database, the SIP AS, the HTPP Server, the HTTP Client, and the Floor Control Server.
- The IUT (MCPTT Server) is the acting Participating Server and Controlling Server

Preamble:

- The IUT (MCPTT Server) is connected to PLMN1.
- The IUT (MCPTT Server) is connected to the SS-UE1 (MCPTT client) as defined in TS 36.579-1 [2], Figure 4.2.4.

5.1.3.2 Test procedure sequence

Table 5.1.3.2-1: Main behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
0A	The SS-UE1 (MCPTT client) sends an HTTP GET (initial UE configuration) request to retrieve the initial UE configuration from the Server.	<--	HTTP GET	-	-
0B	Check: Does the IUT (MCPTT Server) respond by sending an HTTP 200 (OK) including the initial UE configuration document?	-->	HTTP 200 (OK)	1	P
0C	The SS-UE1 (MCPTT client) establishes a secure TLS tunnel as specified by 3GPP TS 33.310 [23] to the authorisation endpoint of the IdM server as specified in 3GPP TS 33.180 [24] using the configured URL of the authorisation endpoint of the IdM server as specified in the "<x>/OnNetwork/AppServerInfo/IDMSAuthEndpoint" leaf node, Table 5.5.8.1-1, TS 36.579-1 [2].	-	-	-	-
1	The SS-UE1 (MCPTT client) sends an OpenID Connect Authentication Request using HTTP POST	<--	HTTP POST (Authorization)	-	-
2	Check: Does the IUT (MCPTT Server) respond by sending an HTTP 200 (OK) including the HTML form requesting username and password?	-->	HTTP 200 (OK)	1	P
3	The SS-UE1 (MCPTT client) sends an HTTP POST Request message to the SS containing user name and password	<--	HTTP POST	-	-
4	Check: Does the IUT (MCPTT Server) send an HTTP 302 (Found) as the OpenID Connect Authentication Response?	-->	HTTP 302 (Found)	1	P
5	The SS-UE1 (MCPTT client) establishes a secure TLS tunnel as specified by 3GPP TS 33.310 [23] to the token endpoint of the IdM server as specified in 3GPP TS 33.180 [24] using the configured URL of the token endpoint of the IdM server as specified in the "/<x>/OnNetwork/AppServerInfo/IDMSTokenEndpoint" leaf node, Table 5.5.8.1-1, TS 36.579-1 [2]	-	-	-	-
6	The SS-UE1 (MCPTT client) sends an HTTP POST Request message to the IUT (MCPTT Server) over the TLS connection established to the IdM token endpoint (OIDC Token Request message) passing the authorization code sent in step 4.	<--	HTTP POST	-	-
7	Check: Does the IUT (MCPTT Server) send an HTTP 200 (OK) providing id_token, access_token and refresh token?	-->	HTTP 200 (OK)	1	P
7A	The SS-UE1 (MCPTT client) establishes a secure TLS tunnel as specified by 3GPP TS 33.310 [23] to the HTTP Proxy as specified in 3GPP TS 33.180 [24] using the configured URL of the HTTP Proxy as specified in the "/<x>/OnNetwork/AppServerInfo/HTTPproxy" leaf node, Table 5.5.8.1-1, TS 36.579-1 [2]	-	-	-	-
8	The SS-UE1 (MCPTT client) sends an HTTP POST message presenting an access token sent in step 7 for Key Management Initialisation.	<--	HTTP POST	-	-
9	Check: Does the IUT (MCPTT Server) respond by sending identity-specific key information?	-->	HTTP 200 (OK)	2	P
10	The SS-UE1 (MCPTT client) sends an HTTP POST message presenting an access token for Key Material Request	<--	HTTP POST	-	-
11	Check: Does the IUT (MCPTT Server) respond by sending identity-specific key information?	-->	HTTP 200 (OK)	2	P

12	The SS-UE1 (MCPTT client) sends a SIP REGISTER request for service authorisation	<--	SIP REGISTER	-	-
13	Check: Does the IUT (MCPTT Server) respond by sending an SIP 200 (OK) message?	-->	SIP 200 (OK)	3	P
14	The SS-UE1 (MCPTT client) sends a SIP SUBSCRIBE - subscription to multiple documents simultaneously - containing the access token and a resource list mime body containing a list of the following documents: MCPTT UE Configuration document, MCPTT User Profile Configuration Document, and the MCPTT Service configuration document. The base URI of each list entry is set to the CMS XCAP-ROOT-URI	<--	SIP SUBSCRIBE	-	-
15	Check: Does the IUT (MCPTT Server) respond by sending an SIP 200 (OK) message?	-->	SIP 200 (OK)	4	P
16	Check: Does the IUT (MCPTT Server) send a SIP NOTIFY message containing the XCAP-URI of the documents?	-->	SIP NOTIFY	4	P
17	The SS-UE1 (MCPTT client) responds with a SIP 200 (OK) message	<--	SIP 200 (OK)	-	-
18	The SS-UE1 (MCPTT client) sends an HTTP GET Request message that contains the access token and the XCAP-URI of the MCPTT UE Configuration document	<--	HTTP GET	-	-
19	Check: Does the IUT (MCPTT Server) send the HTTP 200 (OK) message including the MCPTT UE Configuration Document?	-->	HTTP 200 (OK)	4	P
20	The SS-UE1 (MCPTT client) sends an HTTP GET Request message that contains the access token and the XCAP-URI of the MCPTT User Profile Configuration Document	<--	HTTP GET	-	-
21	Check: Does the IUT (MCPTT Server) send the HTTP 200 (OK) message including the MCPTT User Profile Configuration Document?	-->	HTTP 200 (OK)	4	P
22	The SS-UE1 (MCPTT client) sends an HTTP GET Request message that contains the access token and the XCAP-URI of the MCPTT Service Configuration Document	<--	HTTP GET	-	-
23	Check: Does the IUT (MCPTT Server) send the HTTP 200 (OK) message including the MCPTT Service Configuration Document?	-->	HTTP 200 (OK)	4	P
24	The SS-UE1 (MCPTT client) sends a SIP SUBSCRIBE containing the access token and a resource list mime body and a list of the Groups to be obtained. The base URI of each list entry is set to the GMS XCAP-ROOT-URI, and the MCPTT group ID identifies a group document	<--	SIP SUBSCRIBE	-	-
25	Check: Does the IUT (MCPTT Server) respond with a HTTP 200 (OK) message	-->	SIP 200 (OK)	5	P
26	Check: Does the IUT (MCPTT Server) send a SIP NOTIFY message to the UE that contains the XCAP-URI of the Group documents?	-->	SIP NOTIFY	5	P
27	The SS-UE1 (MCPTT client) sends a SIP 200 (OK) message	<--	SIP 200 (OK)	-	-
28	The SS-UE1 (MCPTT client) sends an HTTP GET Request message that contains the access token and the XCAP-URI of the Group Configuration document	<--	HTTP GET	-	-
29	Check: Does the IUT (MCPTT Server) send an HTTP 200 (OK) message including the Group Document 'MCPTT UE Configuration document'?	-->	HTTP 200 (OK)	5	P

29A	Check: Does the IUT (MCPTT Server) send a SIP NOTIFY message to the UE that contains the group key transport payloads (GKTP) document.	-->	SIP NOTIFY	5	P
29B	The SS-UE1 (MCPTT client) sends a SIP 200 (OK) message	<--	SIP 200 (OK)	-	-
30	The SS-UE1 (MCPTT client) sends a SIP PUBLISH request for update of PoC-settings. NOTE: The PoC-settings document contains the user profile index of the selected user profile.	<--	SIP PUBLISH	-	-
31	Check: Does the IUT (MCPTT Server) send a SIP 200 (OK)?	-->	SIP 200 (OK)	6	P
32-33	Void	--	-	-	-

5.1.3.3 Specific message contents

Table 5.1.3.3-1: HTTP POST (Step 1, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.3-1, condition AUTH

Table 5.1.3.3-2: HTTP POST (Step 3, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.3-1, condition USERAUTH

Table 5.1.3.3-3: HTTP POST (Step 6, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.3-1, condition TOKEN

Table 5.1.3.3-4: HTTP POST (Step 8, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.3-1, condition KMSINIT.

Table 5.1.3.3-5: HTTP POST (Step 10, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.3-1, condition KMSKEY.

Table 5.1.3.3-5A: HTTP 200 (OK) (Step 0B, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1, condition UEINITIALCONFIG

Table 5.1.3.3-6: HTTP 200 (OK) (Step 2, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Content-Type				
media-type	"text/html"		RFC 2854 [111]	
Message-body				
HTML form	<!DOCTYPE html> <html> <body> <form action="/idms/userauth" method="post"> Username: <input type="text" name="user"> Password: <input type="password" name="password"> <button type="submit">Login</button> </form> </body> </html>	"/idms/userauth" given by tsc_MCX_IdMS_userauth_UriPath is the URI to be used by the UE as request URI in the HTTP POST request for user authentication	HTML 4.01 Specification [105]	

Table 5.1.3.3-7: HTTP 200 (OK) (Step 7, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1, condition TOKEN

Table 5.1.3.3-8: HTTP 200 (OK) (Step 9, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1, condition KMSINIT.

Table 5.1.3.3-9: HTTP 200 (OK) (Step 11, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1, condition KMSKEY.

Table 5.1.3.3-10: HTTP 200 (OK) (Step 19, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1, condition UECONFIG.

Table 5.1.3.3-11: HTTP 200 (OK) (Step 21, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1, condition UEUSERPROF.

Table 5.1.3.3-12: HTTP 200 (OK) (Step 23, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1, condition UESERVCONFIG.

Table 5.1.3.3-13: HTTP 200 (OK) (Step 29, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.6-1, condition GROUPCONFIG.

Table 5.1.3.3-14: HTTP 302 (Found) (Step 4, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.8-1, condition AUTH.

Table 5.1.3.3-14A: HTTP GET (Step 0A, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.2-1, condition UEINITIALCONFIG

Table 5.1.3.3-15: HTTP GET (Step 18, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.2-1, condition UECONFIG.

Table 5.1.3.3-16: HTTP GET (Step 20, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.2-1, condition UEUSERPROF.

Table 5.1.3.3-17: HTTP GET (Step 22, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.2-1, condition UESERVCONFIG.

Table 5.1.3.3-18: HTTP GET (Step 28, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.4.2-1, condition GROUPCONFIG

Table 5.1.3.3-19: SIP REGISTER (Step 12, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.13-1, condition SIP_REGISTER_INITIAL, CONFIG				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	SIP URI of the home domain name		

Table 5.1.3.3-20: SIP SUBSCRIBE (Step 14, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.14-1, condition CONFIG

Table 5.1.3.3-20A: SIP SUBSCRIBE (Step 24, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.14-1, condition GROUPCONFIG				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Message-body				
MIME body part		**Resource lists**		
MIME-part-body	Resource-lists as described in Table 5.1.3.3-20B			

Table 5.1.3.3-20B: Resource-lists in SIP SUBSCRIBE (Table 5.1.3.3-20A)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.3.1-1, condition GROUPCONFIG

Table 5.1.3.3-21: SIP NOTIFY (Step 16, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.8-1, condition CONFIG				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B			

Table 5.1.3.3-21A: SIP NOTIFY (Step 26, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.8-1, condition GROUPCONFIG				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B			

Table 5.1.3.3-21B: SIP NOTIFY (Step 29A, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.8-1, condition GROUPCONFIG				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B			
Message-body				
xcap-diff document	xcap-diff document as described in Table 5.1.3.3-21C			

Table 5.1.3.3-21C: Xcap-Diff Document (Table 5.1.3.3-21B)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.12-2, condition GROUPKEY

Table 5.1.3.3-22: SIP PUBLISH (Step 30, Table 5.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.11-1, condition POC-SETTINGS-EVENT				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	The public service identity identifying the originating participating MCPTT function serving the MCPTT user		

Table 5.1.3.3-23: Void

Table 5.1.3.3-24: SIP 200 (OK) (Steps 13, Table 5.1.3.2-1))

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition REGISTER-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**

Table 5.1.3.3-25: SIP 200 (OK) (Steps 15, 25, Table 5.1.3.2-1))

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition SUBSCRIBE-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B			

Table 5.1.3.3-26: SIP 200 (OK) (Step 31, Table 5.1.3.2-1))

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition PUBLISH-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**

6 MCPTT Server - MCPTT Client operation

6.1 MCPTT Server - MCPTT Client / On-demand Pre-arranged Group Call / Automatic Commencement Mode / Floor Control

6.1.1 Test Purpose (TP)

(1)

```
with { IUT (MCPTT Server) connected to PLMN1 }
ensure that {
  when { the SS-UE1 (MCPTT client ) or SS-UE2 (MCPTT client) initiates registration }
    then { IUT (MCPTT Server) initially responds with a SIP 401 Unauthorized message and continues
the process by responding to the SS-UE1 (MCPTT client) or SS-UE2 (MCPTT client) with SIP 200 (OK)
messages }
            }
```

(2)

```
with { IUT (MCPTT Server) having registered the clients}
ensure that {
  when { the SS (MCPTT Client) initiates a pre-arranged group call with automatic commencement mode
}
    then { IUT (MCPTT Server) accepts the call from the initiator and establishes the call with all
registered users of the group }
            }
```

(3)

```
with { IUT (MCPTT Server) having established an MCPTT On-demand Pre-arranged Group Call with
Automatic Commencement Mode }
ensure that {
  when { the SS-UE1 (MCPTT client) or SS-UE2 (MCPTT client) engages in communication }
    then { IUT (MCPTT Server) enforces floor control (Floor Taken, Floor Ack, Floor Idle, Floor
Granted, Floor Queue Position Info, Floor Deny, Floor Revoke) }
            }
```

(4)

```
with { IUT (MCPTT Server) having established an MCPTT On-demand Pre-arranged Group Call with
Automatic Commencement Mode }
ensure that {
  when { the SS-UE1 (MCPTT client) ends the pre-arranged group call }
    then { IUT (MCPTT Server) responds by sending a SIP 200 (OK) message to the client ending the
call and sends a SIP BYE message to the other participants }
            }
```

6.1.2 Conformance requirements

References: The conformance requirements covered in the present TC are specified in: TS 24.379 clause 10.1.1.3.1.1, 10.1.1.3.2, 6.3.2.1.6, 6.3.2.2.8.1, TS 24.380 clause 6.3.2.2, 6.3.5.2.2, 6.3.5.3.3, 6.3.5.5.3, 6.3.5.5.4, 6.3.5.3.5, 6.3.5.5.5, 6.3.5.4.4, 6.3.5.4.7. Unless otherwise stated these are Rel-13 requirements.

[TS 24.379 clause 10.1.1.3.1.1]

In the procedures in this subclause:

1) group identity in an incoming SIP INVITE request refers to the group identity from the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request;

2) emergency indication in an incoming SIP INVITE request refers to the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

3) imminent peril indication in an incoming SIP INVITE request refers to the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body.

Upon receipt of a "SIP INVITE request for originating participating MCPTT function" containing an application/vnd.3gpp.mcptt-info+xml MIME body with the <session-type> element set to a value of "prearranged", the participating MCPTT function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCPTT function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [24]. Otherwise, continue with the rest of the steps;

NOTE 1: if the SIP INVITE request contains an emergency indication or an imminent peril indication set to a value of "true" and this is an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1, the participating MCPTT function can according to local policy choose to accept the request.

2) shall determine the MCPTT ID of the calling user from public user identity in the P-Asserted-Identity header field of the SIP INVITE request, and shall authorise the calling user;

NOTE 2: The MCPTT ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if through local policy in the participating MCPTT function, the user identified by the MCPTT ID is not authorised to initiate prearranged group calls, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "109 user not authorised to make prearranged group calls" in a Warning header field as specified in subclause 4.4;

4) shall validate the media parameters and if the MCPTT speech codec is not offered in the SIP INVITE request shall reject the request with a SIP 488 (Not Acceptable Here) response. Otherwise, continue with the rest of the steps;

5) shall check if the number of maximum simultaneous MCPTT group calls supported for the MCPTT user as specified in the <MaxSimultaneousCallsN6> element of the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.384 [50]) has been exceeded. If exceeded, the participating MCPTT function shall respond with a SIP 486 (Busy Here) response with the warning text set to "103 maximum simultaneous MCPTT group calls reached" in a Warning header field as specified in subclause 4.4. Otherwise, continue with the rest of the steps;

NOTE 3: If the SIP INVITE request contains an emergency indication or an imminent peril indication, the participating MCPTT function can by means beyond the scope of this specification choose to allow for an exception to the limit for the maximum simultaneous MCPTT sessions supported for the MCPTT user. Alternatively, a lower priority session of the MCPTT user could be terminated to allow for the new session.

6) if the user identified by the MCPTT ID is not affiliated to the group identified in the "SIP INVITE request for originating participating MCPTT function" as determined by subclause 9.2.2.2.11 and this is an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1, shall perform the actions specified in subclause 9.2.2.2.12 for implicit affiliation;

7) if the actions for implicit affiliation specified in step 6) above were performed but not successful in affiliating the MCPTT user due to the MCPTT user already having N2 simultaneous affiliations, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 486 (Busy Here) response with the warning text set to "102 too many simultaneous affiliations" in a Warning header field as specified in subclause 4.4. and skip the rest of the steps.

NOTE 4: N2 is the total number of MCPTT groups that an MCPTT user can be affiliated to simultaneously as specified in 3GPP TS 23.179 [3].

NOTE 5: if the SIP INVITE request contains an emergency indication set to a value of "true" or an imminent peril indication set to a value of "true" and this is an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1, the participating MCPTT function can according to local policy choose to allow an exception to the N2 limit. Alternatively, a lower priority affiliation of the MCPTT user could be cancelled to allow for the new affiliation.

8) shall determine the public service identity of the controlling MCPTT function associated with the group identity in the SIP INVITE request;

NOTE 6: The public service identity can identify the controlling MCPTT function in the primary MCPTT system or a partner MCPTT system.

NOTE 7: How the participating MCPTT server discovers the public service identity of the controlling MCPTT function associated with the group identity is out of scope of the current release.

9) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.3;

10) shall set the Request-URI to the public service identity of the controlling MCPTT function associated with the group identity which was present in the incoming SIP INVITE request;

11) shall not copy the following header fields from the incoming SIP INVITE request to the outgoing SIP INVITE request, if they were present in the incoming SIP INVITE request:

   a) Answer-Mode header field as specified in IETF RFC 5373 [18]; and

   b) Priv-Answer-Mode header field as specified in IETF RFC 5373 [18];

12) shall set the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request to the MCPTT ID of the calling user;

13) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the MCPTT client as specified in subclause 6.3.2.1.1.1;

14) if the received SIP INVITE request contains an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in clause F.3 and if not already copied, shall copy the contents of the application/vnd.3gpp.mcptt-location-info+xml MIME body received in the SIP INVITE request into an application/vnd.3gpp.mcptt-location-info+xml MIME body included in the outgoing SIP request;

15) if a Resource-Priority header field was included in the received SIP INVITE request, shall include a Resource-Priority header field according to rules and procedures of 3GPP TS 24.229 [4] set to the value indicated in the Resource-Priority header field of the SIP INVITE request from the MCPTT client; and

NOTE 8: The participating MCPTT function will leave verification of the Resource-Priority header field to the controlling MCPTT function.

16) shall forward the SIP INVITE request, according to 3GPP TS 24.229 [4].

Upon receipt of a SIP 302 (Moved Temporarily) response to the above SIP INVITE request, the participating MCPTT function:

1) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.10;

2) shall include an SDP offer based upon the SDP offer in the received SIP INVITE request from the MCPTT client as specified in subclause 6.3.2.1.1.1; and

3) shall forward the SIP INVITE request according to 3GPP TS 24.229 [4].

Upon receipt of a SIP 2xx response in response to the above SIP INVITE request, the participating MCPTT function:

1) if the received SIP 2xx response contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <MKFC-GKTPs> element, shall perform the procedures in subclause 6.3.2.3.2;

2) shall generate a SIP 200 (OK) response as in subclause 6.3.2.1.5.2;

3) shall include in the SIP 200 (OK) response an SDP answer as specified in the subclause 6.3.2.1.2.1;

4) shall include Warning header field(s) that were received in the incoming SIP 200 (OK) response;

5) shall include the public service identity received in the P-Asserted-Identity header field of the incoming SIP 200 (OK) response into the P-Asserted-Identity header field of the outgoing SIP 200 (OK) response;

6) shall include an MCPTT session identity mapped to the MCPTT session identity provided in the Contact header field of the received SIP 200 (OK) response;

7) if the procedures of subclause 9.2.2.2.12 for implicit affiliation were performed in the present subclause, shall complete the implicit affiliation by performing the procedures of subclause 9.2.2.2.13;

8) shall send the SIP 200 (OK) response to the MCPTT client according to 3GPP TS 24.229 [4];

9) shall interact with Media Plane as specified in 3GPP TS 24.380 [5]; and

10) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [7].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request, the participating MCPTT function:

1) shall generate a SIP response according to 3GPP TS 24.229 [4];

2) shall include Warning header field(s) that were received in the incoming SIP response;

3) shall forward the SIP response to the MCPTT client according to 3GPP TS 24.229 [4]; and

4) if the implicit affiliation procedures of subclause 9.2.2.2.12 were invoked in this procedure, shall perform the procedures of subclause 9.2.2.2.14;

[TS 24.379 clause 10.1.1.3.2]

In the procedures in this subclause:

1) emergency indication in an incoming SIP INVITE request refers to the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

2) imminent peril indication in an incoming SIP INVITE request refers to the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body.

This subclause covers both on-demand session and pre-established sessions.

Upon receipt of a "SIP INVITE request for terminating participating MCPTT function", the participating MCPTT function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCPTT function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [24], and shall not continue with the rest of the steps;

NOTE: if the SIP INVITE request contains an emergency indication or an imminent peril indication set to a value of "true" and this is an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1, the participating MCPTT function can according to local policy choose to accept the request.

2) shall check the presence of the isfocus media feature tag in the URI of the Contact header field and if it is not present then the participating MCPTT function shall reject the request with a SIP 403 (Forbidden) response with the warning text set to "104 isfocus not assigned" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

3) if the Answer-Mode Indication in the application/poc-settings+xml MIME body has not yet been received from the invited MCPTT client as defined in subclause 7.3.3 or subclause 7.3.4, shall reject the request with a SIP 480 (Temporarily Unavailable) response with the warning text set to "146 T-PF unable to determine the service settings for the called user" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

4) shall use the MCPTT ID present in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request to retrieve the binding between the MCPTT ID and public user identity;

5) if the binding between the MCPTT ID and public user identity does not exist, then the participating MCPTT function shall reject the SIP INVITE request with a SIP 404 (Not Found) response. Otherwise, continue with the rest of the steps;

6) if the SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <MKFC-GKTPs> element, shall perform the procedures in subclause 6.3.2.3.2;

7) shall perform the automatic commencement procedures specified in subclause 6.3.2.2.5.1 and according to IETF RFC 5373 [18] if the "SIP INVITE request for terminating participating MCPTT function" does not contain an Answer-Mode header field and the Answer-Mode Indication received in the application/poc-settings+xml MIME body received from the invited MCPTT client as per subclause 7.3.3 or subclause 7.3.4 is set to "auto-answer"; and

8) shall perform the manual commencement procedures specified in subclause 6.3.2.2.6.1 and according to IETF RFC 5373 [18] if the "SIP INVITE request for terminating participating MCPTT function" does not contain an Answer-Mode header field and the Answer-Mode Indication received in the application/poc-settings+xml MIME body received from the invited MCPTT client as per subclause 7.3.3 or subclause 7.3.4 is set to "manual-answer".

[TS 24.379 clause 6.3.2.1.6]

Upon receiving a SIP BYE request from the MCPTT client, the participating MCPTT function:

1) shall interact with the media plane as specified in subclause 6.4 in 3GPP TS 24.380 [5];

2) shall generate a SIP BYE request as specified in 3GPP TS 24.229 [4];

3) shall set the Request-URI to the MCPTT session identity as included in the received SIP BYE request;

4) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP BYE request to the P-Asserted-Identity header field of the outgoing SIP BYE request; and

5) shall send the SIP BYE request toward the controlling MCPTT function, according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the SIP BYE request the terminating MCPTT function shall forward a SIP 200 (OK) response to the MCPTT client and shall interact with the media plane as specified in subclause 6.4 in 3GPP TS 24.380 [5] for releasing media plane resources associated with the SIP session with the controlling MCPTT function.

[TS 24.379 clause 6.3.2.2.8.1]

Upon receiving a SIP BYE request from the controlling MCPTT function, the participating MCPTT function:

1) shall interact with the media plane as specified in subclause 6.4 in 3GPP TS 24.380 [5] for releasing media plane resource associated with the SIP session with the controlling MCPTT function;

2) shall generate a SIP BYE request according to 3GPP TS 24.229 [4];

3) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP BYE request to the P-Asserted-Identity header field of the outgoing SIP BYE request; and

4) shall send the SIP BYE request to the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the SIP BYE request the participating MCPTT function:

1) shall send a SIP 200 (OK) response to the SIP BYE request received from the controlling MCPTT function according to 3GPP TS 24.229 [4]; and

2) shall interact with the media plane as specified in 3GPP TS 24.380 [5] for releasing media plane resources associated with the SIP session with the MCPTT client.

[TS 24.380, clause 6.3.2.2]

When an MCPTT call is established a new instance of the floor control server state machine for 'general floor control operation' is created.

For each MCPTT client added to the MCPTT call, a new instance of the floor control server state machine for 'basic floor control operation towards the floor participant' is added.

If the optional "mc_queueing" feature is supported and has been negotiated as specified in clause 14, the floor control server could queue the implicit floor control request for the media-floor control entity.

The original initial SIP INVITE request or SIP REFER request to establish an MCPTT chat group call or to rejoin an ongoing MCPTT call is not handled as an implicit floor control request message by the floor control server unless explicitly stated in the SIP INVITE request or in the SIP REFER request.

The permission to send media to the inviting MCPTT client due to implicit floor control request is applicable to both confirmed indication and unconfirmed indication.

When the first unconfirmed indication is received from the invited participating MCPTT function (see 3GPP TS 24.379 [2]) the floor control server optionally can give an early indication to send RTP media packets, to the inviting MCPTT client.

If an early indication to send RTP media packets is given to the inviting MCPTT client, the floor participant is granted the permission to send media and the MCPTT server buffers RTP media packets received from the MCPTT client at least until the first invited MCPTT client accepts the invitation or until the RTP media packet buffer exceeds it maximum limit to store RTP media packets.

If the MCPTT server does not support or does not allow media buffering then when an early indication to send RTP media packets is not given to the inviting MCPTT client, the floor participant is granted the permission to send media when the first invited MCPTT client accepts the media.

Before the floor control server sends the first floor control message in the MCPTT call, the floor control server has to assign itself a SSRC identifier to be included in media floor control messages and quality feedback messages if the MCPTT server is supporting that option. A suitable algorithm to generate the SSRC identifier is described in IETF RFC 3550 [3].

The floor participant and the floor control server can negotiate the maximum priority level that the floor participant is permitted to request. The floor control server can pre-empt the current sender based on the negotiated maximum priority level that the floor participant is permitted to request and the priority level included in the Floor Request message.

NOTE: The maximum priority level that a floor participant can use is negotiated as specified in subclause 14.3.3 and is based on group configuration data retrieved by the controlling MCPTT function from the group management server as described in 3GPP TS 24.381 [12] and service configuration data retrieved by the controlling MCPTT function from the configuration management server as described in 3GPP TS 24.384 [13].

The floor participant and the floor control server can negotiate queuing of floor requests using the "mc_queueing" fmtp attribute as described in clause 14. If queuing is supported and negotiated, the floor control server queues the floor control request if a Floor Request message is received when another floor participant has the floor and the priority of the current speaker is the same or higher.

[TS 24.380, clause 6.3.5.2.2]

When a SIP Session is established and if the session is not a temporary group call session or if the session is a temporary group call session and the associated floor participant is an invited MCPTT client (i.e. not a constituent MCPTT group):

NOTE 1: A MCPTT group call is a temporary group session when the <on-network-temporary> element is present in the <list-service> element as specified in 3GPP TS 24.381 [12].

1. if an MCPTT client initiates an MCPTT call with an implicit floor request, and the MCPTT call does not exist yet, the floor control interface towards the MCPTT client in the floor control server:

   a. shall initialize a general state machine as specified in subclause 6.3.4.2.2; and

NOTE 2: In the subclause 6.3.4.2.2 the 'general floor control operation' state machine will continue with the initialization of the 'general floor control operation' state machine.

   b. shall enter the state 'U: permitted' as specified in the subclause 6.3.5.5.2;

2. if the associated MCPTT client rejoins an ongoing MCPTT call without an implicit floor request or initiates or joins a chat group call without an implicit floor request or attempts to initiate an already existing MCPTT call without an implicit floor request, and

   a. if an MCPTT call already exists but no MCPTT client has the permission to send a media, the floor control interface towards the MCPTT client in the floor control server:

      i. should send a Floor Idle message to the MCPTT client. The Floor Idle message:

         A. shall include a Message Sequence Number field with a Message Sequence Number value increased with 1; and

         B. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

      ii. shall enter the state 'U: not permitted and Floor Idle' as specified in the subclause 6.3.5.5.2;

   b. if an MCPTT call is initiated, the floor control interface towards the MCPTT client in the floor control server:

      i. shall enter the state 'U: not permitted and Floor Idle' as specified in the subclause 6.3.5.5.2; and

      ii. shall initialize a general state machine as specified in subclause 6.3.4.2.2; and

NOTE 3: In the subclause 6.3.4.2.2 the general state machine will continue with the initialization of the general state machine.

   c. if another MCPTT client has the permission to send a media, the floor control interface towards the MCPTT client in the floor control server:

      i. should send a Floor Taken message to the MCPTT client. The Floor Taken message:

         A. shall include the granted MCPTT users MCPTT ID in the Granted Party's Identity field, if privacy is not requested;

         B. shall include a Message Sequence Number field with a <Message Sequence Number> value increased with 1;

         C. if the session is a broadcast group call, shall include the Permission to Request the floor field set to '0';

         D. if the session is not a broadcast group call, may include the Permission to Request the floor field set to '1'; and

         E. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications

      ii. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2;

3. if the associated floor participant attempts to initiate an already existing MCPTT call with an implicit floor request, and

   a. if no MCPTT client has the permission to send media, the floor control interface towards the MCPTT client in the floor control server:

      i. shall processes the implicit floor request as if a Floor Request message was receive as specified in subclause 6.3.4.3.3; and

ii. shall enter the state 'U: permitted' as specified in the subclause 6.3.5.5.2;

b. if the MCPTT client negotiated support of queuing floor requests as specified in clause 14 and if another MCPTT client has the permission to send media, the floor control interface towards the MCPTT client in the floor control server:

i. shall set the priority level to the negotiated maximum priority level that the MCPTT client is permitted to request, except for pre-emptive priority, when high priority is used;

NOTE 4: The maximum floor priority the floor participant is permitted to request is negotiated in the "mc_priority" fmtp attribute as specified in clause 14.

NOTE 5: The initial implicit floor request will not result in pre-emption when an MCPTT client is joining an ongoing MCPTT call. If the MCPTT client wants to pre-empt the current MCPTT client that are sending media, an explicit floor request with pre-emptive floor priority is required.

ii. shall insert the MCPTT client into the active floor request queue to the position immediately following all queued floor requests with the same floor priority;

iii. shall send a Floor Queue Position Info message to the MCPTT client. The Floor Queue Position Info message:

A shall include the queue position and floor priority in the Queue Info field; and

B. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications;

iv. should send a Floor Queue Position Info message with the updated status to the MCPTT clients in the active floor request queue which negotiated queuing of floor requests as specified in clause 14, which have requested the queue status, whose queue position has been changed since the previous Floor Queue Position Info message and which is not the joining MCPTT client. The Floor Queue Position Info message:

A shall include the queue position and floor priority in the Queue Info field; and

B. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

v. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2; and

c. if the MCPTT client did not negotiate queuing of floor requests and if another MCPTT client has the permission to send a media, the floor control interface towards the MCPTT client in the floor control server:

i. shall send a Floor Taken message to the MCPTT client. The Floor Taken message:

A. shall include the granted MCPTT users MCPTT ID in the Granted Party's Identity field, if privacy is not requested;

B. shall include a Message Sequence Number field with a Message Sequence Number value increased with 1;

C. if the session is a broadcast group call, shall include the Permission to Request the floor field set to '0';

D. if the session is not a broadcast group call, may include the Permission to Request the floor field set to '1'; and

E. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

ii. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2; and

4. if the MCPTT client is invited to the MCPTT call and

a. if another MCPTT client has permission to send a media, the floor control interface towards the MCPTT client in the floor control server:

i. should send a Floor Taken message to the MCPTT client. The Floor Taken message:

A. shall include the granted MCPTT users MCPTT ID in the Granted Party's Identity field, if privacy is not requested;

B. shall include a Message Sequence Number field with a Message Sequence Number value increased with 1;

C. if the session is a broadcast group call, shall include the Permission to Request the floor field set to '0';

D. if the session is not a broadcast group call, may include the Permission to Request the floor field set to '1'; and

E. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

ii. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2; and

b. if no other MCPTT client has the permission to send a media; the floor control interface towards the MCPTT client in the floor control server:

i. should send a Floor Idle message to the MCPTT client. The Floor Idle message:

A. shall include a Message Sequence Number field with a <Message Sequence Number> value increased with 1; and

B. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

ii. shall enter the 'U: not permitted and Floor Idle' state as specified in the subclause 6.3.5.3.2.

When a SIP Session is established and if the session is a temporary group call session and,

1. if the associated floor participant is a constituent MCPTT group; or

2. if the associated floor participant is the initiator of the temporary group session;

then the floor control interface towards the MCPTT client:

1. shall initialize a general state machine as specified in subclause 6.3.4.2.2, if not already initiated; and

2. shall enter the 'U: not permitted and initiating' state as specified in subclause 6.3.5.10.2.

[TS 24.380, clause 6.3.5.3.3]

When a Floor Taken message is received from the floor control server arbitration logic, the floor control interface towards the MCPTT client in the floor control server:

1. shall forward the Floor Taken message to the associated floor participant;

2. may set the first bit in the subtype of the Floor Taken message to '1' (Acknowledgment is required) as described in subclause 8.3.2, and

NOTE: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

3. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2.

[TS 24.380, clause 6.3.5.5.3]

Upon receiving a Floor Release message from the associated floor participant, the floor control interface towards the MCPTT client in the floor control server:

1. if the first bit in the subtype of the Floor Release message is set to '1' (Acknowledgment is required) as described in subclause 8.3.2, shall send a Floor Ack message. The Floor Ack message:

a. shall include the Message Type field set to '4' (Floor Release); and

b. shall include the Source field set to '2' (the controlling MCPTT function is the source);

2. if an indication that the participant is overriding without revoke is stored,

   a. shall forward the Floor Release message to the dual floor control operation state machine of the floor control arbitration logic in the MCPTT server with the first bit in the subtype of the Floor Release message set to '0' (Acknowledgment is not required), if not already set;

   b. shall remove the indication that the participant is overriding without revoke; and

   c. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2;

3. if an indication that the participant is overridden without revoke is stored,

   a. shall forward the Floor Release message to the general floor control operation state machine of the floor control arbitration logic in the MCPTT server with the first bit in the subtype of the Floor Release message set to '0' (Acknowledgment is not required), if not already set;

   b. shall remove the indication that the participant is overridden without revoke; and

   c. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2; and

4. if no indication is stored:

   a. shall forward the Floor Release message to the general floor control operation state machine of the floor control arbitration logic in the MCPTT server with the first bit in the subtype of the Floor Release message set to '0' (Acknowledgment is not required), if not already set; and

   b. shall remain in the 'U: permitted' state.

[TS 24.380, clause 6.3.5.5.4]

Upon receiving the Floor Idle message from the floor control server arbitration logic in the MCPTT server, the floor control interface towards the MCPTT client in the floor control server:

1. if the G-bit in the Floor Indicator is set to '1' (Dual Floor) and an indication that the participant is overridden without revoke is stored

   a. shall send Floor Idle message to the associated floor participant;

   b. shall remove the indication that a participant is overridden without revoke; and

   c. shall remain in 'U: permitted state';

2. if no indication is stored shall enter the 'U: not permitted and Floor Idle' state as specified in the subclause 6.3.5.3.2; and

3. if an indication that the participant is overriding without revoke is stored

   a. shall send Floor Idle message to the associated floor participant;

   b. shall remove the indication that a participant is overriding without revoke; and

   c. shall remain in 'U: permitted state'.

[TS 24.380, clause 6.3.5.3.5]

When a Floor Granted message is received from the floor control arbitration logic in the MCPTT server, the floor control interface towards the MCPTT client in the floor control server:

1. shall forward the Floor Granted messages to the associated floor participant;

2. may set the first bit in the subtype of the Floor Granted message to '1' (Acknowledgment is required) as described in subclause 8.3.2; and

NOTE: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

3. shall enter the state 'U: permitted' as specified in subclause 6.3.5.5.2.

[TS 24.380, clause 6.3.5.5.5]

When receiving the Floor Revoke message from the floor control server arbitration logic in the MCPTT server, the floor control interface towards the MCPTT client in the floor control server:

1. shall forward the Floor Revoke message to the floor participant;

2. if the Floor Revoke message includes the Track Info field, shall store the Track Info field; and

3. shall enter the state 'U pending Floor Revoke' as specified in the subclause 6.3.5.6.2.

[TS 24.380, clause 6.3.5.4.4]

Upon receiving a Floor Request message, without a Floor Indicator field or with the Floor Indicator field included where the D-bit (Emergency call) and the E-bit (Imminent peril call) are set to '0', from the associated floor participant, and if the MCPTT client did not negotiate queuing of floor requests or did not include a priority in the "mc_priority" fmtp attribute as specified in clause 14, the floor control interface towards the MCPTT client in the floor control server:

1. shall send a Floor Deny message to the associated floor participant. The Floor Deny message:

   a. shall include in the Reject Cause field the <Reject Cause> value cause #1 (Another MCPTT client has permission);

   b. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value;

   c. if the Floor Request included a Track Info field, shall include the received Track Info field; and

   d. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications;

2. may set the first bit in the subtype of the Floor Deny message to '1' (Acknowledgment is required) as described in subclause 8.3.2; and

NOTE 1: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

3. shall remain in the 'U: not permitted and Floor Taken' state.

Upon receiving a Floor Request message from the associated floor participant and the session is a broadcast group call, the floor control interface towards the MCPTT client in the floor control server:

1. shall send a Floor Deny message to the associated floor participant. The Floor Deny message:

   a. shall include in the Reject Cause field the <Reject Cause> value cause #5 (Receive only);

   b. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value; and

   c. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications;

2. may set the first bit in the subtype of the Floor Deny message to '1' (Acknowledgment is required) as described in subclause 8.3.2; and

NOTE 2: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

3. shall remain in the 'U: not permitted and Floor Taken' state.

Upon receiving a Floor Request message from the associated floor participant and if the MCPTT client negotiated support of queuing of floor requests or included a floor priority in the "mc_priority" or both as described in specified in clause 14 and according to local policy, the floor control interface towards the MCPTT client in the floor control server:

1. shall determine the effective priority level as described in subclause 4.1.1.4 by using the following parameters:

   a. the floor priority shall be:

i. the lower of the floor priority included in Floor Request message and the negotiated maximum floor priority that the MCPTT client is permitted to request, if the MCPTT client negotiated floor priority "mc_priority" and floor priority is included in the Floor Request message;

ii. the receive only floor priority, if the MCPTT client negotiated floor priority in the "mc_priority" fmtp attribute and if the negotiated maximum floor priority that the MCPTT client is permitted to request is "receive only";

iii. the default priority, if the MCPTT client negotiated floor priority in the "mc_priority" fmtp attribute, if the negotiated maximum floor priority that the MCPTT client is permitted to request is not receive only and if the floor priority is not included in the Floor Request message; and

iv. the default priority, if the MCPTT client did not negotiate floor priority in the "mc_priority" fmtp attribute; and

b. the type of the call shall be

i. if the Floor Indicator field is included in the message and the D-bit (Emergency call bit) is set to '1', determined to be an emergency call;

ii. if the Floor Indicator field is included in the message and the E-bit (Imminent peril call) is set to '1', determined to be an imminent peril call; and

iii. if the Floor Indicator field is not included in the message or the Floor Indicator field is included and neither the D-bit (Emergency call bit) nor the E-bit (Imminent peril call) is set to '1', determined to be a normal call;

2. if the effective priority is "receive only", the floor control interface towards the MCPTT client in the floor control server:

a. shall send a Floor Deny message to the floor participant. The Floor Deny message:

i. shall include in the Reject Cause field the <Reject Cause> value cause #5 (Receive only) ;

ii. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value;

iii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

iv. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

b. shall remain in the 'U: not permitted and Floor Taken' state;

3. if

a. a Track Info field is included in the Floor Request message, shall use the topmost <Participant Reference> value and the SSRC in the received Floor Request message to check if the floor participant has a queued floor request; or

b. a Track Info field is not included in the Floor Request message, shall use the SSRC in the received Floor Request message to check if the floor participant has a queued floor request;

4. if the floor participant already has a queued floor request with the same effective priority level, the floor control interface towards the MCPTT client in the floor control server:

a. shall send a Floor Queue Position Info message to the requesting MCPTT client, if the MCPTT client negotiated support of queuing of floor requests as specified in clause 14. The Floor Queue Position Info message:

i. shall include the queue position and floor priority in the Queue Info field;

ii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

iii. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

b. shall remain in the 'U: not permitted and Floor Taken' state

5. if the effective priority level is pre-emptive and there are no other pre-emptive requests in the active floor request queue and the effective priority level of the current MCPTT client with permission to send a media is not the pre-emptive priority, the floor control interface towards the MCPTT client in the floor control server:

   a. shall forward the Floor Request message to the floor control server arbitration logic indicating that a Floor Request message with pre-emptive priority is received; and

   b. shall remain in the 'U: not permitted and Floor Taken' state

NOTE 3: The Floor control server arbitration logic initiates revoking the permission to send media towards the current MCPTT client with the permission to send media as specified in the subclause 6.3.4.4.7;

6. if the MCPTT client did not negotiate support of queuing of floor requests as specified in clause 14, the effective priority level is pre-emptive and either other pre-emptive request is queued or the effective priority level of the current MCPTT client with permission to send a media is the pre-emptive priority, the floor control interface towards the MCPTT client in the floor control server:

   a. shall send a Floor Deny message to the associated floor participant. The Floor Deny message:

      i. shall include in the Reject Cause field the <Reject Cause> value cause #1 (Another MCPTT client has permission);

      ii. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value;

      iii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

      iv. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

   b. shall remain in the 'U: not permitted and Floor Taken' state;

7. if the MCPTT client did not negotiate "queuing" and the effective priority level is not pre-emptive, the floor control interface towards the MCPTT client in the floor control server:

   a. shall send a Floor Deny message to the associated floor participant. The Floor Deny message:

      i. shall include in the Reject Cause field the <Reject Cause> value cause #1 (Another MCPTT client has permission);

      ii. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value;

      iii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

      iv. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

   b. shall remain in the 'U: not permitted and Floor Taken' state; and

8. if the MCPTT client negotiated support of queuing of floor requests as specified in clause 14 and the effective priority level is not pre-emptive, the floor control interface towards the MCPTT client in the floor control server:

   a. shall insert the MCPTT client into the active floor request queue, if not inserted yet, or update the position of the MCPTT client in the active floor request queue, if already inserted, to the position immediately following all queued requests at the same effective priority level;

   b. the floor control server shall send a Floor Queue Position Info message to the floor participant. The Floor Queue Position Info message:

      i. shall include the queue position and floor priority in the Queue Info field;

      ii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

iii. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications;

c. shall remain in the 'U: not permitted and Floor Taken' state; and

d. may set the first bit in the subtype of the Floor Queue Position message to '1' (Acknowledgment is required) as described in subclause 8.3.2.

NOTE 4: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

[TS 24.380, clause 6.3.5.4.7]

Upon receiving a Floor Queue Position Request message from the associated floor participant, the floor control interface towards the MCPTT client in the floor control server:

1. shall send the Floor Queue Position Info message. The Floor Queue Position Info message:

   a. shall include the queue position and floor priority in the Queue Info field;

   b. if a Track Info field is included in the Floor Queue Position Info message, shall include the received Track Info field;

   c. may include the first bit in the subtype of the Floor Queue Position Info message set to '1' (Acknowledgment is required) as described in subclause 8.3.2; and

NOTE: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

   d. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

3. shall remain in the 'U: not permitted and Floor Taken' state.

6.1.3 Test description

6.1.3.1 Pre-test conditions

System Simulator:

- SS-UE1 (MCPTT client)
- SS-UE2 (MCPTT client)
- For the underlying "transport bearer" over which the SS-UE1 (MCPTT client) and SS-UE2 (MCPTT client) and the MCPTT Server will communicate, Parameters are set to the default parameters for the basic E-UTRA Single cell network scenarios, as defined in 3GPP TS 36.508 [22] clause 4.4. The simulated Cell 1 shall belong to PLMN1 (the PLMN specified for MCPTT operation in the MCPTT configuration document).

IUT:

- IUT (MCPTT Server)
- The IUT (MCPTT Server) consists of all sub-systems of the Common Services Core, including the Group Management Server, the Configuration Management Server, the Key Management Server, the Identity Management Server, the HTTP Server, and the SIP AS. The IUT (MCPTT Server) also consists of all sub-systems of the MCPTT Server, including the Media Distribution Function, the MCPTT User Database, the SIP AS, the HTPP Server, the HTTP Client, and the Floor Control Server.
- The IUT (MCPTT Server) is the acting Participating Server and Controlling Server

Preamble:

- The IUT (MCPTT Server) is connected to PLMN1

- The IUT (MCPTT Server) is connected to the SS-UE1 (MCPTT client) and the SS-UE2 (MCPTT client) as defined in TS 36.579-1 [2], Figure 4.2.4.

- SS-UE1 (MCPTT client) and SS-UE2 (MCPTT client) are affiliated with Group A

- The IUT (MCPTT Server) is the controlling server for Group A

6.1.3.2 Test procedure sequence

Table 6.1.3.2-1: Main behaviour

St	Procedure	Message Sequence		TP	Verdict
		U – S	Message		
-	EXCEPTION: In parallel to the event described in steps 1 to 4 below the SS-UE1 (MCPTT client) user authentication, authorization, and configuration as according to Table 5.1.3.2-1 takes place.	-	-	-	-
1	The SS-UE1 (MCPTT client) sends initial registration for IMS services.	<--	SIP REGISTER	-	-
2	Check: Does the IUT (MCPTT Server) respond with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network?	-->	SIP 401 Unauthorized	1	P
3	The SS-UE1 (MCPTT client) completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.	<--	SIP REGISTER	-	-
4	Check: Does the IUT (MCPTT Server) send a SIP 200 (OK) to the SS-UE1 (MCPTT client)?	-->	SIP 200 (OK)	1	P
5-6	Void	-	-	-	-
-	EXCEPTION: In parallel to the event described in steps 7 to 10 below the SS-UE2 (MCPTT client) user authentication, authorization, and configuration as according to Table 5.1.3.2-1 takes place.	-	-	-	-
7	The SS-UE2 (MCPTT client) sends initial registration for IMS services.	<--	SIP REGISTER	-	-
8	Check: Does the IUT (MCPTT Server) respond with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network?	-->	SIP 401 Unauthorized	1	P
9	The SS-UE2 (MCPTT client) completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.	<--	SIP REGISTER	-	-
10	Check: Does the IUT (MCPTT Server) send a SIP 200 (OK) to the SS-UE2 (MCPTT client)?	-->	SIP 200 (OK)	1	P
11-12	Void	-	-	-	-
13	The SS-UE1 (MCPTT client) initiates an on-demand pre-arranged group call with automatic commencement mode and implicit floor control.	<--	SIP INVITE	-	-
14	Check: Does the IUT (MCPTT Server) send a SIP 100 Trying message to the SS-UE1 (MCPTT client)?	-->	SIP 100 Trying	2	P
15	Check: Does the IUT (MCPTT Server) send a SIP INVITE to the SS-UE2 (MCPTT client)?	-->	SIP INVITE	2	P
16	The SS-UE2 (MCPTT client) responds with a SIP 200 (OK) message	<--	SIP 200 (OK)	-	-
17	Check: Does the IUT (MCPTT Server) send a SIP ACK to the SS-UE2 (MCPTT client)?	-->	SIP ACK	2	P
18	Check: Does the IUT (MCPTT Server) send a SIP 200 (OK) to the SS-UE1 (MCPTT client)?	-->	SIP 200 (OK)	2	P
19	The SS-UE1 (MCPTT client) responds with a SIP 200 (OK) message	<--	SIP ACK	-	-
20	Check: Does the IUT (MCPTT Server) send a Floor Taken message to the SS-UE2 (MCPTT client) informing the SS-UE2 (MCPTT client) that the floor is taken by SS-UE1 (MCPTT client)?	-->	Floor Taken	3	P
21	The SS-UE1 (MCPTT client) sends a Floor Release message with an acknowledgement required to release the floor	<--	Floor Release	-	-

22	Check: Does the IUT (MCPTT Server) send a Floor Ack message to the SS-UE1 (MCPTT client) to acknowledge the Floor Release message?	-->	Floor Ack	3	P
23	Check: Does the IUT (MCPTT Server) send a Floor Idle message to the SS-UE2 (MCPTT client)?	-->	Floor Idle	3	P
24	Check: Does the IUT (MCPTT Server) send a Floor Idle message to the SS-UE1 (MCPTT client)?	-->	Floor Idle	3	P
25	The SS-UE1 (MCPTT client) sends a Floor Request message	<--	Floor Request	-	-
26	Check: Does the IUT (MCPTT Server) send a Floor Granted message to the SS-UE1 (MCPTT client) with no acknowledgement required?	-->	Floor Granted	3	P
27	Check: Does the IUT (MCPTT Server) send a Floor Taken message to the SS-UE2 (MCPTT client) informing the SS-UE2 (MCPTT client) that the floor is taken by SS-UE1 (MCPTT client)?	-->	Floor Taken	3	P
28	The SS-UE2 (MCPTT client) sends a Floor Request message with a higher priority than SS-UE1 (MCPTT client)	<--	Floor Request	-	-
29	Check: Does the IUT (MCPTT Server) send a Floor Revoke message to the SS-UE1 (MCPTT client)?	-->	Floor Revoke	3	P
30	The SS-UE1 (MCPTT client) sends a Floor Release message	<--	Floor Release	-	-
31	Check: Does the IUT (MCPTT Server) send a Floor Granted message to the SS-UE2 (MCPTT client) with no acknowledgement required?	-->	Floor Granted	3	P
32	Check: Does the IUT (MCPTT Server) send a Floor Taken message to the SS-UE1 (MCPTT client) informing the SS-UE1 (MCPTT client) that the floor is taken by SS-UE2 (MCPTT client)?	-->	Floor Taken	3	P
33	The SS-UE1 (MCPTT client) sends a Floor Request message with a lower priority than SS-UE2 (MCPTT client) and the Floor Indicator F-bit set to 0.	<--	Floor Request	-	-
34	Check: Does the IUT (MCPTT Server) send a Floor Deny message to the SS-UE1 (MCPTT client)?	-->	Floor Deny	3	P
35	The SS-UE1 (MCPTT client) sends a Floor Request message with a lower priority than SS-UE2 (MCPTT client) and the Floor Indicator F-bit set to 1.	<--	Floor Request	-	-
36	Check: Does the IUT (MCPTT Server) send a Floor Queue Position Info message to the SS-UE1 (MCPTT client)?	-->	Floor Queue Position Info	3	P
37	The SS-UE1 (MCPTT client) sends a Floor Queue Position Request	<--	Floor Queue Position Request	-	-
38	Check: Does the IUT (MCPTT Server) send a Floor Queue Position Info message to the SS-UE1 (MCPTT client)?	-->	Floor Queue Position Info	3	P
39	The SS-UE2 (MCPTT client) sends a Floor Release message with no acknowledgement required	<--	Floor Release	-	-
40	Check: Does the IUT (MCPTT Server) send a Floor Granted message to the SS-UE1 (MCPTT client) with no acknowledgement required?	-->	Floor Granted	3	P

41	Check: Does the IUT (MCPTT Server) send a Floor Taken message to the SS-UE2 (MCPTT client) informing the SS-UE2 (MCPTT client) that the floor is taken by SS-UE1 (MCPTT client)?	-->	Floor Taken	3	P
42	The SS-UE1 (MCPTT client) sends a Floor Release message with an acknowledgement required to release the floor	<--	Floor Release	-	-
43	Check: Does the IUT (MCPTT Server) send a Floor Ack message to the SS-UE1 (MCPTT client) to acknowledge the Floor Release message?	-->	Floor Ack	3	P
44	Check: Does the IUT (MCPTT Server) send a Floor Idle message to the SS-UE2 (MCPTT client)?	-->	Floor Idle	3	P
45	Check: Does the IUT (MCPTT Server) send a Floor Idle message to the SS-UE1 (MCPTT client)?	-->	Floor Idle	3	P
46	The SS-UE1 (MCPTT client) sends a SIP BYE request	<--	SIP BYE	-	-
47	Check: Does the IUT (MCPTT Server) respond with a SIP 200 (OK) message	-->	SIP 200 (OK)	4	P
48	Check: Does the IUT (MCPTT Server) send a SIP BYE message to the SS-UE2 (MCPTT client) to end the call?	-->	SIP BYE	4	P
49	SS-UE2 (MCPTT client) responds with a SIP 200 (OK) message	<--	SIP 200 (OK)	-	-

6.1.3.3 Specific message contents

Table 6.1.3.3-1: SIP REGISTER (Step 1, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.13-1 condition SIP_REGISTER_INITIAL				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	SIP URI of the home domain name		

Table 6.1.3.3-2: SIP REGISTER (Steps 3, 9, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.13-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	SIP URI of the home domain name		

Table 6.1.3.3-3: SIP REGISTER (Step 7, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.13-1 condition SIP_REGISTER_INITIAL				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	The public service identity of the MCPTT server under test		
From				
addr-spec				
user-info and host	px_MCX_SIP_PublicUserId_B_1			
Authorization				
username	px_MCX_SIP_PrivateUserId_B			

Table 6.1.3.3-4: Void

Table 6.1.3.3-5: SIP 200 (OK) (Step 4, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition REGISTER-RSP

Table 6.1.3.3-6: SIP 200 (OK) (Step 10, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition REGISTER-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
P-Associated-URI				
addr-spec[1]	SIP URI			
host	px_MCX_SIP_PublicUserId_B_1			

Table 6.1.3.3-7: SIP 200 (OK) (Step 16, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.1-1 condition INVITE-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 6.1.3.3-7A			
MIME body part		**MCPTT-Info**		
MIME-part-body	MCPTT-Info message as described in Table 6.1.3.3-7B			

Table 6.1.3.3-7A: SDP in SIP 200 (OK) (Table 6.1.3.3-7)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.1-1 condition SDP_ANSWER

Table 6.1.3.3-7B: MCPTT-Info in SIP 200 (OK) (Table 6.1.3.3-7)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.1-1 conditions GROUP-CALL, INVITE-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
mcpttinfo				
mcptt-Params				
mcptt-calling-user-id	not present			
mcptt-called-party-id	encrypted <mcptt-called-party-id> with mcpttURI set to px_MCPTT_ID_User_B	Encrypted element as described in TS 36.579-1 [2] Table 5.5.3.2.1-1A		

Table 6.1.3.3-8: SIP 200 (OK) (Step 18, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition INVITE-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 6.1.3.3-8A			

Table 6.1.3.3-8A: SDP in SIP 200 (OK) (Table 6.1.3.3-8)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.2-1 conditions SDP_ANSWER, IMPLICIT_FLOOR_GRANTED, IMPLICIT_GRANT_REQUESTED

Table 6.1.3.3-9: Void

Table 6.1.3.3-10: SIP INVITE (Step 13, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.5.1-1 condition MCPTT				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	The public service identity of the MCPTT server under test		
Session-Expires			RFC 4028 [30]	
generic-param	"1800"	The recommended initial value is 1800 in RFC 4028 [30].		
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 6.1.3.3-10A			
MIME body part		**MCPTT-Info**		
MIME-part-body	MCPTT-Info message as described in Table 6.1.3.3-10B			

Table 6.1.3.3-10A: SDP in SIP 200 (OK) (Table 6.1.3.3-10)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.1-1 conditions SDP_OFFER, IMPLICIT_GRANT_REQUESTED

Table 6.1.3.3-10B: MCPTT-Info in SIP 200 (OK) (Table 6.1.3.3-10)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.1-1 conditions GROUP-CALL, INVITE_REFER

Table 6.1.3.3-11: SIP INVITE (Step 15, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.5.2-1 condition MCPTT				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
From				
addr-spec	tsc_MCPTT_PublicServiceId_B			
To				
addr-spec	px_MCX_SIP_PublicUserId_B_1	Default public user ID (IMPU) as stored in the UICC		
Contact				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 6.1.3.3-11A			
MIME body part		**MCPTT-Info**		
MIME-part-body	MCPTT-Info message as described in Table 6.1.3.3-11B			

Table 6.1.3.3-11A: SDP in SIP 200 (OK) (Table 6.1.3.3-11)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.2-1 conditions INITIAL_SDP_OFFER, SDP_OFFER

Table 6.1.3.3-11B: MCPTT_Info in SIP 200 (OK) (Table 6.1.3.3-11)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.2-1 conditions GRPUP-CALL

Table 6.1.3.3-11C: SIP BYE (Step 46, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.2.1-1 condition MO_CALL

Table 6.1.3.3-11D: SIP BYE (Step 48, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.2.2-1 condition MT_CALL				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
P-Asserted-Identity				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B	The URI of the SS		

Table 6.1.3.3-12: Floor Taken (Steps 20, 27, 41, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.7-1 condition ON-NETWORK			
Information Element	**Value/remark**	**Comment**	**Condition**
Granted Party's Identity			
Granted Party's Identity	px_MCPTT_ID_User_A		

Table 6.1.3.3-13: Floor Taken (Step 32, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.7-1 condition ON-NETWORK

Table 6.1.3.3-14: Floor Release (Steps 21, 42, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.5-1 condition ON-NETWORK, ACK			
Information Element	**Value/remark**	**Comment**	**Condition**

Table 6.1.3.3-14A: Floor Ack (Steps 22, 43, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.5-1 condition DOWNLINK			
Information Element	**Value/remark**	**Comment**	**Condition**
Message Type			
Message Type	"00010100"	Acknowledgement for Floor Release message	

Table 6.1.3.3-15: Floor Release (Steps 30, 39, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.5-1 condition ON-NETWORK

Table 6.1.3.3-16: Void

Table 6.1.3.3-17: Floor Request (Steps 25, 35, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.2-1 condition ON-NETWORK			
Information Element	**Value/remark**	**Comment**	**Condition**
Floor priority	"0"	The lowest priority	

Table 6.1.3.3-18: Floor Request (Step 33, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.2-1 condition ON-NETWORK			
Information Element	**Value/remark**	**Comment**	**Condition**
Floor priority	"0"	The lowest priority	
Floor Indicator			
Floor Indicator	"1000000000000000"	bit A=1 (Normal call) bit F=0 (Queuing not supported)	

Table 6.1.3.3-19: Floor Request (Step 28, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.2-1 condition ON-NETWORK			
Information Element	**Value/remark**	**Comment**	**Condition**
Floor priority	"12"		

Table 6.1.3.3-20: Floor Granted (Steps 26, 40, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.3-1 condition ON-NETWORK

Table 6.1.3.3-21: Floor Granted (Step 31, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.3-1 condition ON-NETWORK			
Information Element	**Value/remark**	**Comment**	**Condition**
Floor priority	"12"		

Table 6.1.3.3-22: Void

Table 6.1.3.3-23: Floor Deny (Step 34, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.4-1 condition ON-NETWORK

Table 6.1.3.3-24: Floor Queue Position Info (Steps 36, 38, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.10-1 condition ON-NETWORK

Table 6.1.3.3-25: Floor Queue Position Request (Step 37, Table 6.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.9-1 condition ON-NETWORK

7 MCPTT Server - MCPTT Server operation

7.1 MCPTT Server - MCPTT Server / On-demand Pre-arranged Group Call / Automatic Commencement Mode / Floor Control / Controlling Server

7.1.1 Test Purpose (TP)

(1)

```
with { IUT (MCPTT Server) connected to SS (MCPTT Server) }
ensure that {
  when { the SS-UE2 (MCPTT client) initiates a pre-arranged group call with automatic commencement
mode }
    then { IUT (MCPTT Server) interacts with SS (MCPTT Server) to set up the call by sending SIP
messages }
            }
```

(2)

```
with { IUT (MCPTT Server) having established an MCPTT On-demand Pre-arranged Group Call with
Automatic Commencement Mode }
ensure that {
  when { the SS-UE1 (MCPTT client) and SS-UE2 (MCPTT client) engage in communication }
    then { IUT (MCPTT Server) enforces floor control (Floor Taken, Floor Idle, Floor Granted ) by
sending messages via the SS (MCPTT Server) }
            }
```

(3)

```
with { IUT (MCPTT Server) having established an MCPTT On-demand Pre-arranged Group Call with
Automatic Commencement Mode }
ensure that {
  when { the SS-UE1 (MCPTT client) ends the pre-arranged group call }
    then { IUT (MCPTT Server) responds via the SS (MCPTT Server) by sending a SIP 200 (OK) message
to the client ending the call and sends a SIP BYE message to the other participants }
            }
```

7.1.2 Conformance requirements

References: The conformance requirements covered in the present TC are specified in: TS 24.379 clause 6.3.3.2.3.1, 6.3.3.2.2, 10.1.1.4.2, 6.3.3.1.2, 6.3.3.3, 10.1.1.4.1.2, 6.3.3.2.3.2, 10.1.1.4.1.1, 6.3.3.2.4, 6.3.3.1.5, TS 24.380 clause

6.3.2.2, 6.3.5.2.2, 6.3.5.3.3, 6.3.5.5.3, 6.3.5.5.4, 6.3.5.3.5, 6.3.5.4.4. Unless otherwise stated these are Rel-13 requirements.

[TS 24.379 clause 6.3.3.2.3.1]

When sending SIP provisional responses with the exception of the SIP 100 (Trying) response to the SIP INVITE request the controlling MCPTT function:

1) shall generate the SIP provisional response;

2) shall include a P-Asserted-Identity header field with the public service identity of the controlling MCPTT function;

3) shall include an MCPTT session identity in the Contact header field; and

4) shall include the following in the Contact header field:

   a) the g.3gpp.mcptt media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

   c) the isfocus media feature tag.

[TS 24.379 clause 6.3.3.2.2]

On receipt of an initial SIP INVITE request the controlling MCPTT function shall cache SIP feature tags, if received in the Contact header field and if the specific feature tags are supported.

[TS 24.379 clause 10.1.1.4.2]

In the procedures in this subclause:

1) MCPTT ID in an incoming SIP INVITE request refers to the MCPTT ID of the originating user from the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request;

2) group identity in an incoming SIP INVITE request refers to the group identity from the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request;

3) MCPTT ID in an outgoing SIP INVITE request refers to the MCPTT ID of the called user in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the outgoing SIP INVITE request;

4) indication of required group members in a SIP 183 (Session Progress) response refers to the <required> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to "true" in a SIP 183 (Session Progress) sent by the non-controlling MCPTT function of an MCPTT group;

5) emergency indication in an incoming SIP INVITE request refers to the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

6) imminent peril indication in an incoming SIP INVITE request refers to the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body.

Upon receipt of a "SIP INVITE request for controlling MCPTT function of an MCPTT group", the controlling MCPTT function:

…

2) shall determine if the media parameters are acceptable and the MCPTT speech codec is offered in the SDP offer and if not reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

…

5) shall retrieve the necessary group document(s) from the group management server for the group identity contained in the SIP INVITE request and carry out initial processing as specified in subclause 6.3.5.2;

…

7) shall perform the actions as described in subclause 6.3.3.2.2;

8) shall maintain a local counter of the number of SIP 200 (OK) responses received from invited members and shall initialise this local counter to zero;

9) shall determine if an MCPTT group call for the group identity is already ongoing by determining if an MCPTT session identity has already been allocated for the group call and the MCPTT session is active;

…

13) if the MCPTT group call is not ongoing then:

a) if:

i) the user identified by the MCPTT ID is not affiliated to the group identity contained in the SIP INVITE request as specified in subclause 6.3.6;

ii) the group identity contained in the SIP INVITE request is not a constituent MCPTT group ID;

iii) the received SIP INVITE request does not contain an emergency indication or imminent peril indication; or

iv) the received SIP INVITE request is an authorised request for an MCPTT emergency group call as determined by subclause 6.3.3.1.13.2 or MCPTT imminent peril group call as determined by steps subclause 6.3.3.1.13.5 and is determined to not be eligible for implicit affiliation as specified in subclause 9.2.2.3.6;

then shall return a SIP 403 (Forbidden) response with the warning text set to "120 user is not affiliated to this group" in a Warning header field as specified in subclause 4.4, and skip the rest of the steps below;

…

e) shall create a prearranged group session and allocate an MCPTT session identity for the prearranged group call, and shall handle timer TNG3 (group call timer) as specified in subclause 6.3.3.5;

…

g) if the group identity in the SIP INVITE request for controlling MCPTT function of an MCPTT group is an MCPTT group ID:

i) shall determine the members to invite to the prearranged MCPTT group call as specified in subclause 6.3.5.5;

ii) if necessary, shall start timer TNG1 (acknowledged call setup timer) according to the conditions stated in subclause 6.3.3.3;

…

v) shall invite each group member determined in step 13)g)i) above, to the group session, as specified in subclause 10.1.1.4.1.1; and

vi) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3; and

…

Upon receiving a SIP 183 (Session Progress) response to the SIP INVITE request specified in subclause 10.1.1.4.1 containing a P-Answer-State header field with the value "Unconfirmed" as specified in IETF RFC 4964 [34], the timer TNG1 (acknowledged call setup timer) is not running, the controlling MCPTT function supports media buffering and the SIP final response is not yet sent to the inviting MCPTT client:

1) shall generate a SIP 200 (OK) response to SIP INVITE request as specified in the subclause 6.3.3.2.3.2;

…

3) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP INVITE request as specified in the subclause 6.3.3.2.1;

4) shall include a P-Answer-State header field with the value "Unconfirmed";

…

7) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3;

NOTE 7: Resulting user plane processing is completed before the next step is performed.

8) shall send the SIP 200 (OK) response towards the inviting MCPTT client according to 3GPP TS 24.229 [4];

…

Upon:

1) receiving a SIP 200 (OK) response for a SIP INVITE request as specified in subclause 10.1.1.4.1;

2) the timer TNG1 (acknowledged call setup timer) is not running;

3) the local counter of the number of SIP 200 (OK) responses received from invited members is equal to the value of the <on-network-minimum-number-to-start> element of the group document;

4) the controlling MCPTT function supports media buffering; and

5) the SIP final response has not yet been sent to the inviting MCPTT client;

the controlling MCPTT function according to local policy:

1) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.3.2.2;

…

3) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP INVITE request as specified in the subclause 6.3.3.2.1;

…

6) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3;

NOTE 11:Resulting media plane processing is completed before the next step is performed.

7) shall send a SIP 200 (OK) response to the inviting MCPTT client according to 3GPP TS 24.229 [4];

[TS 24.379 clause 6.3.3.1.2]

This subclause is referenced from other procedures.

The controlling MCPTT function shall generate an initial SIP INVITE request according to 3GPP TS 24.229 [4].

The controlling MCPTT function:

1) shall include in the Contact header field an MCPTT session identity for the MCPTT session with the g.3gpp.mcptt media feature tag, the isfocus media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" according to IETF RFC 3840 [16];

2) shall include an Accept-Contact header field containing the g.3gpp.mcptt media feature tag along with the "require" and "explicit" header field parameters according to IETF RFC 3841 [6];

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [4]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [9] in the SIP INVITE request;

4) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" along with parameters "require" and "explicit" according to IETF RFC 3841 [6];

5) shall include a Referred-By header field with the public user identity of the inviting MCPTT client;

6) should include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [7]. The refresher parameter shall be omitted;

7) shall include the Supported header field set to "timer";

8) shall include an unmodified Priv-Answer-Mode header field if present in the incoming SIP INVITE request;

9) if a Priv-Answer-Mode header field was not present in the incoming SIP INVITE request, shall include an unmodified Answer-Mode header field if present in the incoming SIP INVITE request; and

10) if the incoming SIP INVITE request contained an application/vnd.3gpp.mcptt-info+xml MIME body, shall copy the application/vnd.3gpp.mcptt-info+xml MIME body to the outgoing INVITE request.

[TS 24.379 clause 6.3.3.3]

When the controlling MCPTT function receives a SIP INVITE request to initiate a group session and there are members of the group document retrieved from the group management server that are affiliated and are marked as <on-network-required> as specified in 3GPP TS 24.381 [31], then the controlling MCPTT function shall start timer TNG1 (acknowledged call setup timer) with a timer value as described in Annex B.2.1, prior to sending out SIP INVITE requests inviting group members to the group session.

When the controlling MCPTT function receives all SIP 200 (OK) responses to the SIP INVITE requests, from all affiliated and <on-network-required> members then the controlling MCPTT function shall stop timer TNG1 (acknowledged call setup timer) and if the local counter of the number of SIP 200 (OK) responses received from invited members is greater than or equal to the value of the <on-network-minimum-number-to-start> element of the group document, the controlling MCPTT function shall send a SIP 200 (OK) response to the initiating MCPTT client.

NOTE 1: MCPTT clients that are affiliated but are not <on-network-required> members that have not yet responded will be considered as joining an ongoing session when the controlling MCPTT function receives SIP 200 (OK) responses from these MCPTT clients.

[TS 24.379 clause 10.1.1.4.1.2]

The controlling MCPTT function:

1) shall generate a SIP INVITE request as specified in subclause 6.3.3.1.2;

2) shall set the Request-URI to the public service identity of the non-controlling MCPTT function serving the group identity of the MCPTT group owned by the partner MCPTT system;

3) shall set the P-Asserted-Identity to the public service identity of the controlling MCPTT function;

4) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP INVITE request:

   a) the <mcptt-request-uri> element set to the group identity of the MCPTT group hosted by the non-controlling MCPTT function in the partner MCPTT system; and

   b) the <mcptt-calling-group-id> element set to the group identity of the group served by the controlling MCPTT function;

5) shall include the Recv-Info header field set to g.3gpp.mcptt-floor-request;

6) if:

   a) an MCPTT GKTP document exists for the group identity contained in the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request; and

   b) the MCPTT GKTP document contains a <MKFC-GKTPs> element;

then:

   a) for each instance of <GKTP> element of the <MKFC-GKTPs> element of the MCPTT GKTP document:

      i) shall perform the procedure in subclause 6.3.3.6.2 to re-generate an I_MESSAGE; and

      ii) if the procedure in subclause 6.3.3.6.2 was successful, shall include the I_MESSAGE in a <GKTP> element of the <MKFC-GKTPs> element of an application/vnd.3gpp.mcptt-info+xml MIME body included in the outgoing SIP INVITE request;

7) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the originating network according to the procedures specified in subclause 6.3.3.1.1; and

8) shall send the SIP INVITE request towards the partner MCPTT system in accordance with 3GPP TS 24.229 [4].

Upon receiving SIP 403 (Forbidden) response for the SIP INVITE request, if according to local policy and if:

1) the response contains a Warning header field with the MCPTT warning code "128"; and

2) the response contains a P-Refused-URI-List header field and an application/resource-lists+xml MIME body as specified in IETF RFC 5318 [36];

NOTE 1: The application/resource-lists+xml MIME body contains MCPTT IDs identifying MCPTT users in a partner MCPTT system that needs to be invited to the prearranged group call in case of group regrouping using interrogating method as specified in 3GPP TS 23.179 [3] subclause 10.6.2.4.2.

then the controlling MCPTT function:

1) shall check if the number of members of the MCPTT group exceeds the value contained in the <on-network-max-participant-count> element of the group document as specified in 3GPP TS 24.381 [31]. If exceeded, the controlling MCPTT function shall invite only <on-network-max-participant-count> members from the application/resource-lists+xml MIME body; and

NOTE 2: The <on-network-max-participant-count> element indicates the maximum number of participants allowed in the prearranged group session It is operator policy that determines which participants in the application/resource-lists+xml MIME body are invited to the group call.

2) shall invite MCPTT users as specified in this subclause using the list of MCPTT IDs in URI-List.

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the controlling MCPTT function:

1) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3;

NOTE 3: The procedures executed by the controlling MCPTT function prior to sending a response to the inviting MCPTT client are specified in subclause 10.1.1.4.2.

2) if at least one of the invited MCPTT clients has subscribed to the conference package, shall subscribe to the conference event package in the non-controlling MCPTT function as specified in subclause 10.1.3.4.3; and

3) if the 200 (OK) response includes the <floor-state> element set to "floor-taken", shall wait for a SIP INFO request containing a floor request from the non-controlling MCPTT function.

Upon receiving a SIP INFO request containing a floor request where:

1) the Request-URI contains an MCPTT session ID identifying an ongoing temporary group session; and

2) the application/vnd.3gpp.mcptt-info+xml MIME body contains the <mcptt-calling-group-id> element with the MCPTT group ID of a MCPTT group invited to the temporary group session;

then the controlling MCPTT function:

1) shall send a SIP 200 (OK) response to the SIP INFO request to the non-controlling MCPTT function as specified in 3GPP TS 24.229 [4]; and

2) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3.

[TS 24.379 clause 6.3.3.2.3.2]

When sending a SIP 200 (OK) response to the initial SIP INVITE request, the controlling MCPTT function:

1) shall generate the SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [4];

2) shall include the Session-Expires header field and start supervising the SIP session according to rules and procedures of IETF RFC 4028 [7], "UAS Behavior". The "refresher" parameter in the Session-Expires header field shall be set to "uac";

3) shall include the option tag "timer" in a Require header field;

4) shall include a P-Asserted-Identity header field with the public service identity of the controlling MCPTT function;

5) shall include a SIP URI for the MCPTT session identity in the Contact header field identifying the MCPTT session at the controlling MCPTT function;

6) shall include the following in the Contact header field:

   a) the g.3gpp.mcptt media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

   c) the isfocus media feature tag;

7) shall include Warning header field(s) received in incoming responses to the SIP INVITE request;

8) shall include the option tag "tdialog" in a Supported header field according to rules and procedures of IETF RFC 4538 [23];

9) shall include the "norefersub" option tag in a Supported header field according to IETF RFC 4488 [22];

10) shall include the "explicitsub" and "nosub" option tags in a Supported header field according to IETF RFC 7614 [35];

11) if:

   a) an MCPTT GKTP document exists for the group identity contained in the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the initial SIP INVITE request; and

   b) the MCPTT GKTP document contains an <MKFC-GKTPs> element;

then:

   a) for each instance of <GKTP> element of the <MKFC-GKTPs> element of the MCPTT GKTP document:

      i) shall perform the procedure in subclause 6.3.3.6.2 to re-generate an I_MESSAGE; and

ii) if the procedure in subclause 6.3.3.6.2 was successful, shall include the I_MESSAGE in a <GKTP> element of the <MKFC-GKTPs> element of an application/vnd.3gpp.mcptt-info+xml MIME body included in a SIP 200 (OK) response; and

12) shall interact with the media plane as specified in 3GPP TS 24.380 [5].

[TS 24.379 clause 10.1.1.4.1.2]

This subclause describes the procedures for inviting an MCPTT user to an MCPTT session. The procedure is initiated by the controlling MCPTT function as the result of an action in subclause 10.1.1.4.2 or as the result of receiving a SIP 403 (Forbidden) response as described in this subclause.

The controlling MCPTT function:

1) shall generate a SIP INVITE request as specified in subclause 6.3.3.1.2;

2) shall set the Request-URI to the public service identity of the terminating participating MCPTT function associated to the MCPTT user to be invited.;

NOTE 1: How the controlling MCPTT function finds the address of the terminating MCPTT participating function is out of the scope of the current release.

NOTE 2: If the terminating MCPTT user is part of a partner MCPTT system, then the public service identity can identify an entry point in the partner network that is able to identify the terminating participating MCPTT function.

3) shall set the P-Asserted-Identity header field to the public service identity of the controlling MCPTT function;

4) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP INVITE request:

a) the <mcptt-request-uri> element set to the MCPTT ID of the terminating user; and

b) the <mcptt-calling-group-id> element set to the group identity;

NOTE 3: The <mcptt-calling-user-id> is already included in the MIME body as a result of calling subclause 6.3.3.1.2 in step 1).

5) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the originating network according to the procedures specified in subclause 6.3.3.1.1;

6) if the in-progress emergency state of the group is set to a value of "true" the controlling MCPTT function:

a) shall include a Resource-Priority header field populated with the values for an MCPTT emergency group call as specified in subclause 6.3.3.1.19;

b) if the received SIP INVITE request contained an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "true":

i) shall include in the outgoing SIP INVITE request in the application/vnd.3gpp.mcptt-info+xml MIME body an <emergency-ind> element set to a value of "true"; and

ii) if the <alert-ind> element is set to "true" in the received SIP INVITE request and the requesting MCPTT user and MCPTT group are authorised for the initiation of MCPTT emergency alerts as determined by the procedures of subclause 6.3.3.1.13.1, shall populate the application/vnd.3gpp.mcptt-info+xml MIME body and the application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in subclause 6.3.3.1.12. Otherwise, shall set the <alert-ind> element to a value of "false"; and

c) if the in-progress imminent peril state of the group is set to a value of "true" shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <imminentperil-ind> element set to a value of "false";

7) if the in-progress emergency state of the group is set to a value of "false" and the in-progress imminent peril state of the group is set to a value of "true", the controlling MCPTT function:

a) shall include a Resource-Priority header field populated with the values for an MCPTT imminent peril group call as specified in subclause 6.3.3.1.19; and

b) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "true";

8) if:

a) an MCPTT GKTP document exists for the group identity contained in the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request; and

b) the MCPTT GKTP document contains a <MKFC-GKTPs> element;

then:

a) for each instance of <GKTP> element of the <MKFC-GKTPs> element of the MCPTT GKTP document:

i) shall perform the procedure in subclause 6.3.3.6.2 to re-generate an I_MESSAGE; and

ii) if the procedure in subclause 6.3.3.6.2 was successful, shall include the I_MESSAGE in a <GKTP> element of the <MKFC-GKTPs> element of an application/vnd.3gpp.mcptt-info+xml MIME body included in the outgoing SIP INVITE request; and

9) shall send the SIP INVITE request towards the terminating network in accordance with 3GPP TS 24.229 [4].

Upon receiving a SIP 183 (Session Progress) response containing a Require header field with the option tag "100rel" and containing a P-Answer-State header field with the value "Unconfirmed" in response to the SIP INVITE request the controlling MCPTT function:

1) shall send a SIP PRACK request towards the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the controlling MCPTT function:

1) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3;

2) shall send a SIP NOTIFY request to all participants with a subscription to the conference event package as specified in subclause 10.1.3.4; and

3) shall increment the local counter of the number of SIP 200 (OK) responses received from invited members, by 1.

NOTE 4: The notifications above could be sent prior to the SIP 200 (OK) response being sent to the inviting MCPTT client. These notifications received by MCPTT clients that are group members do not mean that the group session will be successfully established.

NOTE 5: The procedures executed by the controlling MCPTT function prior to sending a response to the inviting MCPTT client are specified in subclause 10.1.1.4.2.

[TS 24.379 clause 6.3.3.2.4]

Upon receiving a SIP BYE request the controlling MCPTT function:

1) shall interact with the media plane as specified in subclause 6.3 in 3GPP TS 24.380 [5] for releasing the media plane resource associated with the SIP session towards the MCPTT client;

NOTE: The non-controlling MCPTT function is also regarded as a MCPTT client in a temporary MCPTT group session.

2) shall generate a SIP 200 (OK) response and send the SIP response towards the MCPTT client according to 3GPP TS 24.229 [4];

3) shall check the MCPTT session release policy as specified in subclause 6.3.8.1 and subclause 6.3.8.2 whether the MCPTT session needs to be released for each participant of the MCPTT session;

4) if release of the MCPTT session is required, perform the procedures as specified in the subclause 6.3.3.1.5; and

5) if a release of the MCPTT session is not required, shall send a SIP NOTIFY request to all remaining MCPTT clients in the MCPTT session with a subscription to the conference event package as specified in subclause 10.1.3.4.2.

Upon receiving a SIP 200 (OK) response to the SIP BYE request the controlling MCPTT function shall interact with the media plane as specified in subclause 6.3 in 3GPP TS 24.380 [5] for releasing media plane resources associated with the SIP session with the MCPTT participant.

[TS 24.379 clause 6.3.3.1.5]

When a participant needs to be removed from the MCPTT session, the controlling MCPTT function:

1) shall interact with the media plane as specified in 3GPP TS 24.380 [5] for the MCPTT session release;

2) shall generate a SIP BYE request according to 3GPP TS 24.229 [4]; and

3) shall send the SIP BYE request to the MCPTT clients according to3GPP TS 24.229 [4].

If timer TNG3 (group call timer) has not expired, then when the last MCPTT client is removed from the MCPTT session, the controlling MCPTT function shall stop timer TNG3 (group call timer).

When the MCPTT group session needs to be released, the controlling MCPTT function shall send SIP BYE requests as described in this subclause, to all participants of the group session.

Upon receiving a SIP 200 (OK) response to a SIP BYE request the controlling MCPTT function shall interact with the media plane as specified in subclause 6.3 in 3GPP TS 24.380 [5] for releasing media plane resources associated with the SIP session with the MCPTT clients.

[TS 24.380 clause 6.3.2.2]

When an MCPTT call is established a new instance of the floor control server state machine for 'general floor control operation' is created.

For each MCPTT client added to the MCPTT call, a new instance of the floor control server state machine for 'basic floor control operation towards the floor participant' is added.

If the optional "mc_queueing" feature is supported and has been negotiated as specified in clause 14, the floor control server could queue the implicit floor control request for the media-floor control entity.

The original initial SIP INVITE request or SIP REFER request to establish an MCPTT chat group call or to rejoin an ongoing MCPTT call is not handled as an implicit floor control request message by the floor control server unless explicitly stated in the SIP INVITE request or in the SIP REFER request.

The permission to send media to the inviting MCPTT client due to implicit floor control request is applicable to both confirmed indication and unconfirmed indication.

When the first unconfirmed indication is received from the invited participating MCPTT function (see 3GPP TS 24.379 [2]) the floor control server optionally can give an early indication to send RTP media packets, to the inviting MCPTT client.

If an early indication to send RTP media packets is given to the inviting MCPTT client, the floor participant is granted the permission to send media and the MCPTT server buffers RTP media packets received from the MCPTT client at least until the first invited MCPTT client accepts the invitation or until the RTP media packet buffer exceeds it maximum limit to store RTP media packets.

If the MCPTT server does not support or does not allow media buffering then when an early indication to send RTP media packets is not given to the inviting MCPTT client, the floor participant is granted the permission to send media when the first invited MCPTT client accepts the media.

Before the floor control server sends the first floor control message in the MCPTT call, the floor control server has to assign itself a SSRC identifier to be included in media floor control messages and quality feedback messages if the MCPTT server is supporting that option. A suitable algorithm to generate the SSRC identifier is described in IETF RFC 3550 [3].

The floor participant and the floor control server can negotiate the maximum priority level that the floor participant is permitted to request. The floor control server can pre-empt the current sender based on the negotiated maximum priority level that the floor participant is permitted to request and the priority level included in the Floor Request message.

NOTE: The maximum priority level that a floor participant can use is negotiated as specified in subclause 14.3.3 and is based on group configuration data retrieved by the controlling MCPTT function from the group management server as described in 3GPP TS 24.381 [12] and service configuration data retrieved by the controlling MCPTT function from the configuration management server as described in 3GPP TS 24.384 [13].

The floor participant and the floor control server can negotiate queuing of floor requests using the "mc_queueing" fmtp attribute as described in clause 14. If queuing is supported and negotiated, the floor control server queues the floor control request if a Floor Request message is received when another floor participant has the floor and the priority of the current speaker is the same or higher.

[TS 24.380 clause 6.3.5.2.2]

When a SIP Session is established and if the session is not a temporary group call session or if the session is a temporary group call session and the associated floor participant is an invited MCPTT client (i.e. not a constituent MCPTT group):

NOTE 1: A MCPTT group call is a temporary group session when the <on-network-temporary> element is present in the <list-service> element as specified in 3GPP TS 24.381 [12].

1. if an MCPTT client initiates an MCPTT call with an implicit floor request, and the MCPTT call does not exist yet, the floor control interface towards the MCPTT client in the floor control server:

   a. shall initialize a general state machine as specified in subclause 6.3.4.2.2; and

NOTE 2: In the subclause 6.3.4.2.2 the 'general floor control operation' state machine will continue with the initialization of the 'general floor control operation' state machine.

   b. shall enter the state 'U: permitted' as specified in the subclause 6.3.5.5.2;

2. if the associated MCPTT client rejoins an ongoing MCPTT call without an implicit floor request or initiates or joins a chat group call without an implicit floor request or attempts to initiate an already existing MCPTT call without an implicit floor request, and

a. if an MCPTT call already exists but no MCPTT client has the permission to send a media, the floor control interface towards the MCPTT client in the floor control server:

   i. should send a Floor Idle message to the MCPTT client. The Floor Idle message:

      A. shall include a Message Sequence Number field with a Message Sequence Number value increased with 1; and

      B. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

   ii. shall enter the state 'U: not permitted and Floor Idle' as specified in the subclause 6.3.5.5.2;

b. if an MCPTT call is initiated, the floor control interface towards the MCPTT client in the floor control server:

   i. shall enter the state 'U: not permitted and Floor Idle' as specified in the subclause 6.3.5.5.2; and

   ii. shall initialize a general state machine as specified in subclause 6.3.4.2.2; and

NOTE 3: In the subclause 6.3.4.2.2 the general state machine will continue with the initialization of the general state machine.

c. if another MCPTT client has the permission to send a media, the floor control interface towards the MCPTT client in the floor control server:

   i. should send a Floor Taken message to the MCPTT client. The Floor Taken message:

      A. shall include the granted MCPTT users MCPTT ID in the Granted Party's Identity field, if privacy is not requested;

      B. shall include a Message Sequence Number field with a <Message Sequence Number> value increased with 1;

      C. if the session is a broadcast group call, shall include the Permission to Request the floor field set to '0';

      D. if the session is not a broadcast group call, may include the Permission to Request the floor field set to '1'; and

      E. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications

   ii. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2;

3. if the associated floor participant attempts to initiate an already existing MCPTT call with an implicit floor request, and

   a. if no MCPTT client has the permission to send media, the floor control interface towards the MCPTT client in the floor control server:

      i. shall processes the implicit floor request as if a Floor Request message was receive as specified in subclause 6.3.4.3.3; and

      ii. shall enter the state 'U: permitted' as specified in the subclause 6.3.5.5.2;

   b. if the MCPTT client negotiated support of queuing floor requests as specified in clause 14 and if another MCPTT client has the permission to send media, the floor control interface towards the MCPTT client in the floor control server:

      i. shall set the priority level to the negotiated maximum priority level that the MCPTT client is permitted to request, except for pre-emptive priority, when high priority is used;

NOTE 4: The maximum floor priority the floor participant is permitted to request is negotiated in the "mc_priority" fmtp attribute as specified in clause 14.

NOTE 5: The initial implicit floor request will not result in pre-emption when an MCPTT client is joining an ongoing MCPTT call. If the MCPTT client wants to pre-empt the current MCPTT client that are sending media, an explicit floor request with pre-emptive floor priority is required.

ii. shall insert the MCPTT client into the active floor request queue to the position immediately following all queued floor requests with the same floor priority;

iii. shall send a Floor Queue Position Info message to the MCPTT client. The Floor Queue Position Info message:

A shall include the queue position and floor priority in the Queue Info field; and

B. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications;

iv. should send a Floor Queue Position Info message with the updated status to the MCPTT clients in the active floor request queue which negotiated queuing of floor requests as specified in clause 14, which have requested the queue status, whose queue position has been changed since the previous Floor Queue Position Info message and which is not the joining MCPTT client. The Floor Queue Position Info message:

A shall include the queue position and floor priority in the Queue Info field; and

B. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

v. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2; and

c. if the MCPTT client did not negotiate queuing of floor requests and if another MCPTT client has the permission to send a media, the floor control interface towards the MCPTT client in the floor control server:

i. shall send a Floor Taken message to the MCPTT client. The Floor Taken message:

A. shall include the granted MCPTT users MCPTT ID in the Granted Party's Identity field, if privacy is not requested;

B. shall include a Message Sequence Number field with a Message Sequence Number value increased with 1;

C. if the session is a broadcast group call, shall include the Permission to Request the floor field set to '0';

D. if the session is not a broadcast group call, may include the Permission to Request the floor field set to '1'; and

E. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

ii. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2; and

4. if the MCPTT client is invited to the MCPTT call and

a. if another MCPTT client has permission to send a media, the floor control interface towards the MCPTT client in the floor control server:

i. should send a Floor Taken message to the MCPTT client. The Floor Taken message:

A. shall include the granted MCPTT users MCPTT ID in the Granted Party's Identity field, if privacy is not requested;

B. shall include a Message Sequence Number field with a Message Sequence Number value increased with 1;

C. if the session is a broadcast group call, shall include the Permission to Request the floor field set to '0';

D. if the session is not a broadcast group call, may include the Permission to Request the floor field set to '1'; and

E. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

ii. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2; and

b. if no other MCPTT client has the permission to send a media; the floor control interface towards the MCPTT client in the floor control server:

i. should send a Floor Idle message to the MCPTT client. The Floor Idle message:

A. shall include a Message Sequence Number field with a <Message Sequence Number> value increased with 1; and

B. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

ii. shall enter the 'U: not permitted and Floor Idle' state as specified in the subclause 6.3.5.3.2.

When a SIP Session is established and if the session is a temporary group call session and,

1. if the associated floor participant is a constituent MCPTT group; or

2. if the associated floor participant is the initiator of the temporary group session;

then the floor control interface towards the MCPTT client:

1. shall initialize a general state machine as specified in subclause 6.3.4.2.2, if not already initiated; and

2. shall enter the 'U: not permitted and initiating' state as specified in subclause 6.3.5.10.2.

[TS 24.380 clause 6.3.5.3.3]

When a Floor Taken message is received from the floor control server arbitration logic, the floor control interface towards the MCPTT client in the floor control server:

1. shall forward the Floor Taken message to the associated floor participant;

2. may set the first bit in the subtype of the Floor Taken message to '1' (Acknowledgment is required) as described in subclause 8.3.2, and

NOTE: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

3. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2.

[TS 24.380 clause 6.3.5.5.3]

Upon receiving a Floor Release message from the associated floor participant, the floor control interface towards the MCPTT client in the floor control server:

1. if the first bit in the subtype of the Floor Release message is set to '1' (Acknowledgment is required) as described in subclause 8.3.2, shall send a Floor Ack message. The Floor Ack message:

a. shall include the Message Type field set to '4' (Floor Release); and

b. shall include the Source field set to '2' (the controlling MCPTT function is the source);

2. if an indication that the participant is overriding without revoke is stored,

a. shall forward the Floor Release message to the dual floor control operation state machine of the floor control arbitration logic in the MCPTT server with the first bit in the subtype of the Floor Release message set to '0' (Acknowledgment is not required), if not already set;

b. shall remove the indication that the participant is overriding without revoke; and

c. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2;

3. if an indication that the participant is overridden without revoke is stored,

a. shall forward the Floor Release message to the general floor control operation state machine of the floor control arbitration logic in the MCPTT server with the first bit in the subtype of the Floor Release message set to '0' (Acknowledgment is not required), if not already set;

b. shall remove the indication that the participant is overridden without revoke; and

c. shall enter the 'U: not permitted and Floor Taken' state as specified in the subclause 6.3.5.4.2; and

4. if no indication is stored:

a. shall forward the Floor Release message to the general floor control operation state machine of the floor control arbitration logic in the MCPTT server with the first bit in the subtype of the Floor Release message set to '0' (Acknowledgment is not required), if not already set; and

b. shall remain in the 'U: permitted' state.

[TS 24.380 clause 6.3.5.5.4]

Upon receiving the Floor Idle message from the floor control server arbitration logic in the MCPTT server, the floor control interface towards the MCPTT client in the floor control server:

1. if the G-bit in the Floor Indicator is set to '1' (Dual Floor) and an indication that the participant is overridden without revoke is stored

a. shall send Floor Idle message to the associated floor participant;

b. shall remove the indication that a participant is overridden without revoke; and

c. shall remain in 'U: permitted state';

2. if no indication is stored shall enter the 'U: not permitted and Floor Idle' state as specified in the subclause 6.3.5.3.2; and

3. if an indication that the participant is overriding without revoke is stored

a. shall send Floor Idle message to the associated floor participant;

b. shall remove the indication that a participant is overriding without revoke; and

c. shall remain in 'U: permitted state'.

[TS 24.380 clause 6.3.5.3.5]

When a Floor Granted message is received from the floor control arbitration logic in the MCPTT server, the floor control interface towards the MCPTT client in the floor control server:

1. shall forward the Floor Granted messages to the associated floor participant;

2. may set the first bit in the subtype of the Floor Granted message to '1' (Acknowledgment is required) as described in subclause 8.3.2; and

NOTE: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

3. shall enter the state 'U: permitted' as specified in subclause 6.3.5.5.2.

[TS 24.380 clause 6.3.5.4.4]

Upon receiving a Floor Request message, without a Floor Indicator field or with the Floor Indicator field included where the D-bit (Emergency call) and the E-bit (Imminent peril call) are set to '0', from the associated floor participant, and if the MCPTT client did not negotiate queuing of floor requests or did not include a priority in the "mc_priority" fmtp attribute as specified in clause 14, the floor control interface towards the MCPTT client in the floor control server:

1. shall send a Floor Deny message to the associated floor participant. The Floor Deny message:

a. shall include in the Reject Cause field the <Reject Cause> value cause #1 (Another MCPTT client has permission);

b. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value;

c. if the Floor Request included a Track Info field, shall include the received Track Info field; and

d. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications;

2. may set the first bit in the subtype of the Floor Deny message to '1' (Acknowledgment is required) as described in subclause 8.3.2; and

NOTE 1: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

3. shall remain in the 'U: not permitted and Floor Taken' state.

Upon receiving a Floor Request message from the associated floor participant and the session is a broadcast group call, the floor control interface towards the MCPTT client in the floor control server:

1. shall send a Floor Deny message to the associated floor participant. The Floor Deny message:

a. shall include in the Reject Cause field the <Reject Cause> value cause #5 (Receive only);

b. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value; and

c. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications;

2. may set the first bit in the subtype of the Floor Deny message to '1' (Acknowledgment is required) as described in subclause 8.3.2; and

NOTE 2: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

3. shall remain in the 'U: not permitted and Floor Taken' state.

Upon receiving a Floor Request message from the associated floor participant and if the MCPTT client negotiated support of queuing of floor requests or included a floor priority in the "mc_priority" or both as described in specified in clause 14 and according to local policy, the floor control interface towards the MCPTT client in the floor control server:

1. shall determine the effective priority level as described in subclause 4.1.1.4 by using the following parameters:

a. the floor priority shall be:

i. the lower of the floor priority included in Floor Request message and the negotiated maximum floor priority that the MCPTT client is permitted to request, if the MCPTT client negotiated floor priority "mc_priority" and floor priority is included in the Floor Request message;

ii. the receive only floor priority, if the MCPTT client negotiated floor priority in the "mc_priority" fmtp attribute and if the negotiated maximum floor priority that the MCPTT client is permitted to request is "receive only";

iii. the default priority, if the MCPTT client negotiated floor priority in the "mc_priority" fmtp attribute, if the negotiated maximum floor priority that the MCPTT client is permitted to request is not receive only and if the floor priority is not included in the Floor Request message; and

iv. the default priority, if the MCPTT client did not negotiate floor priority in the "mc_priority" fmtp attribute; and

b. the type of the call shall be

i. if the Floor Indicator field is included in the message and the D-bit (Emergency call bit) is set to '1', determined to be an emergency call;

ii. if the Floor Indicator field is included in the message and the E-bit (Imminent peril call) is set to '1', determined to be an imminent peril call; and

iii. if the Floor Indicator field is not included in the message or the Floor Indicator field is included and neither the D-bit (Emergency call bit) nor the E-bit (Imminent peril call) is set to '1', determined to be a normal call;

2. if the effective priority is "receive only", the floor control interface towards the MCPTT client in the floor control server:

   a. shall send a Floor Deny message to the floor participant. The Floor Deny message:

      i. shall include in the Reject Cause field the <Reject Cause> value cause #5 (Receive only) ;

      ii. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value;

      iii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

      iv. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

   b. shall remain in the 'U: not permitted and Floor Taken' state;

3. if

   a. a Track Info field is included in the Floor Request message, shall use the topmost <Participant Reference> value and the SSRC in the received Floor Request message to check if the floor participant has a queued floor request; or

   b. a Track Info field is not included in the Floor Request message, shall use the SSRC in the received Floor Request message to check if the floor participant has a queued floor request;

4. if the floor participant already has a queued floor request with the same effective priority level, the floor control interface towards the MCPTT client in the floor control server:

   a. shall send a Floor Queue Position Info message to the requesting MCPTT client, if the MCPTT client negotiated support of queuing of floor requests as specified in clause 14. The Floor Queue Position Info message:

      i. shall include the queue position and floor priority in the Queue Info field;

      ii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

      iii. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

   b. shall remain in the 'U: not permitted and Floor Taken' state

5. if the effective priority level is pre-emptive and there are no other pre-emptive requests in the active floor request queue and the effective priority level of the current MCPTT client with permission to send a media is not the pre-emptive priority, the floor control interface towards the MCPTT client in the floor control server:

   a. shall forward the Floor Request message to the floor control server arbitration logic indicating that a Floor Request message with pre-emptive priority is received; and

   b. shall remain in the 'U: not permitted and Floor Taken' state

NOTE 3: The Floor control server arbitration logic initiates revoking the permission to send media towards the current MCPTT client with the permission to send media as specified in the subclause 6.3.4.4.7;

6. if the MCPTT client did not negotiate support of queuing of floor requests as specified in clause 14, the effective priority level is pre-emptive and either other pre-emptive request is queued or the effective priority level of the current MCPTT client with permission to send a media is the pre-emptive priority, the floor control interface towards the MCPTT client in the floor control server:

   a. shall send a Floor Deny message to the associated floor participant. The Floor Deny message:

      i. shall include in the Reject Cause field the <Reject Cause> value cause #1 (Another MCPTT client has permission);

ii. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value;

iii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

iv. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

b. shall remain in the 'U: not permitted and Floor Taken' state;

7. if the MCPTT client did not negotiate "queuing" and the effective priority level is not pre-emptive, the floor control interface towards the MCPTT client in the floor control server:

a. shall send a Floor Deny message to the associated floor participant. The Floor Deny message:

i. shall include in the Reject Cause field the <Reject Cause> value cause #1 (Another MCPTT client has permission);

ii. may include in the Reject Cause field an additional text string explaining the reason for rejecting the floor request in the <Reject Phrase> value;

iii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

iv. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications; and

b. shall remain in the 'U: not permitted and Floor Taken' state; and

8. if the MCPTT client negotiated support of queuing of floor requests as specified in clause 14 and the effective priority level is not pre-emptive, the floor control interface towards the MCPTT client in the floor control server:

a. shall insert the MCPTT client into the active floor request queue, if not inserted yet, or update the position of the MCPTT client in the active floor request queue, if already inserted, to the position immediately following all queued requests at the same effective priority level;

b. the floor control server shall send a Floor Queue Position Info message to the floor participant. The Floor Queue Position Info message:

i. shall include the queue position and floor priority in the Queue Info field;

ii. if the Floor Request included a Track Info field, shall include the received Track Info field; and

iii. if a group call is a broadcast group call, a system call, an emergency call, an imminent peril call, or a temporary group session, shall include the Floor Indicator field with appropriate indications;

c. shall remain in the 'U: not permitted and Floor Taken' state; and

d. may set the first bit in the subtype of the Floor Queue Position message to '1' (Acknowledgment is required) as described in subclause 8.3.2.

NOTE 4: It is an implementation option to handle the receipt of the Floor Ack message and what action to take if the Floor Ack message is not received.

7.1.3 Test description

7.1.3.1 Pre-test conditions

System Simulator:

- SS (MCPTT Server)
  - SS (MCPTT Server) provides the participating MCPTT functions
- SS-UE1 (MCPTT client)
- SS-UE2 (MCPTT client)

IUT:

- IUT (MCPTT Server)
  - IUT (MCPTT Server) provides the controlling MCPTT function
- The IUT (MCPTT Server) consists of all sub-systems of the Common Services Core, including the Group Management Server, the Configuration Management Server, the Key Management Server, the Identity Management Server, the HTTP Server, and the SIP AS. The IUT (MCPTT Server) also consists of all sub-systems of the MCPTT Server, including the Media Distribution Function, the MCPTT User Database, the SIP AS, the HTPP Server, the HTTP Client, and the Floor Control Server.

Preamble:

- The IUT (MCPTT Server) is connected to SS (MCPTT Server) defined in TS 36.579-1 [2], Figure 4.2.5.
- SS-UE1 (MCPTT client) and SS-UE2 (MCPTT client) are affiliated with Group A and are authorized to initiate prearranged group calls
- Group A is controlled by the controlling MCPTT function, IUT (MCPTT Server)

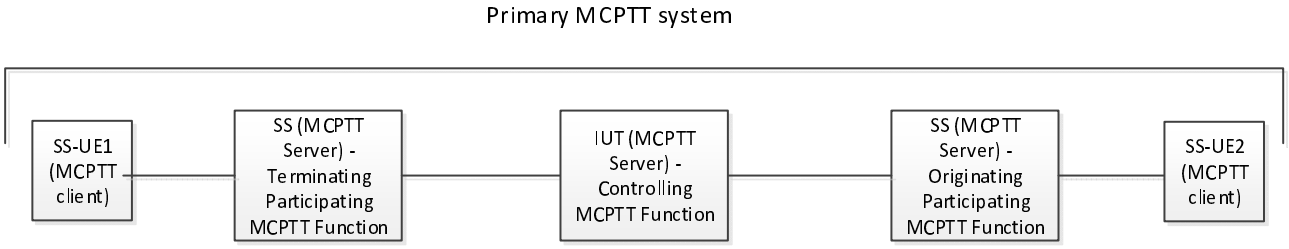

Figure 7.1.3.1-1: Functions of the testing components

7.1.3.2 Test procedure sequence

Table 7.1.3.2-1: Main behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The SS (MCPTT Server) sends a SIP INVITE message initiating a pre-arranged group call with automatic commencement mode from SS-UE2 (MCPTT client) to SS-UE1 (MCPTT client).	<--	SIP INVITE	-	-
2	Check: Does the IUT (MCPTT Server) send a SIP 100 (Trying) message to the participating server SS (MCPTT Server)?	-->	SIP 100 (Trying)	1	P
3	Check: Does the IUT (MCPTT Server) send a SIP INVITE message for SS-UE1 (MCPTT client) to the participating server SS (MCPTT Server)?	-->	SIP INVITE	1	P
4	The SS (MCPTT Server) responds to the SIP INVITE message by sending a SIP 183 (Session Progress) message	<--	SIP 183 (Session Progress)	-	-
5	Check: Does the IUT (MCPTT Server) send a SIP PRACK message to the server SS (MCPTT Server)?	-->	SIP PRACK	1	P
5A	The SS (MCPTT Server) responds to the SIP PRACK with a SIP 200 (OK) message.	<--	SIP 200 OK	-	-
6	Check: Does the IUT (MCPTT Server) send a SIP 200 (OK) message to SS-UE2 (MCPTT Client) via the participating server SS (MCTT Server) with the P-Answer-State header field set to "unconfirmed"?	-->	SIP 200 (OK)	1	P
7	The SS-UE1 (MCPTT Client) responds to the SIP INVITE in step 3 via the SS (MCPTT Server) by sending a SIP 200 (OK) message	<--	SIP 200 OK	-	-
8	Check: Does the IUT (MCPTT Server) respond to the SIP INVITE sent in step 1 with a SIP 200 (OK) message?	-->	SIP 200 (OK)	1	P
9	The SS (MCPTT Server) responds with a SIP ACK message	<--	SIP ACK	-	-
10	Check: The IUT (MCPTT Server) responds to the SS-UE1 (MCPTT Client) via the server SS (MCPTT server) with a SIP ACK message	-->	SIP ACK	1	P
11	Check: Does the IUT (MCPTT Server) send a Floor Taken message to the SS-UE1 (MCPTT client) via the participating server SS (MCPTT Server)?	-->	Floor Taken	2	P
12	The SS (MCPTT Server) sends a Floor Release message with no acknowledgement required to release the floor from SS-UE2 (MCPTT client)	<--	Floor Release	-	-
13	Check: Does the IUT (MCPTT Server) send a Floor Idle message to the SS-UE2 (MCPTT client) via the participating server SS (MCPTT Server)?	-->	Floor Idle	2	P
14	Check: Does the IUT (MCPTT Server) send a Floor Idle message to the SS-UE1 (MCPTT client) via the participating server SS (MCPTT Server)?	-->	Floor Idle	2	P
15	The SS (MCPTT Server) sends a Floor Request message from SS-UE1 (MCPTT client)	<--	Floor Request	-	-
16	Check: Does the IUT (MCPTT Server) send a Floor Granted message to the SS-UE1 (MCPTT client) via the participating server SS (MCPTT Server)?	-->	Floor Granted	2	P
17	Check: Does the IUT (MCPTT Server) send a Floor Taken message to the SS-UE2 (MCPTT client) via the participating server SS (MCPTT Server)?	-->	Floor Taken	2	P

18	The SS (MCPTT Server) sends a Floor Release message from SS-UE1 (MCPTT client)	<--	Floor Release	-	-
19	Check: Does the IUT (MCPTT Server) send a Floor Idle message to the SS-UE1 (MCPTT client) via the participating server SS (MCPTT Server)?	-->	Floor Idle	2	P
20	Check: Does the IUT (MCPTT Server) send a Floor Idle message to the SS-UE2 (MCPTT client) via the participating server SS (MCPTT Server)?	-->	Floor Idle	2	P
21	The SS (MCPTT Server) sends a SIP BYE request from SS-UE1 (MCPTT client)	<--	SIP BYE	-	-
22	Check: Does the IUT (MCPTT Server) respond with a SIP 200 (OK) message to SS-UE1 (MCPTT client) via the participating server SS (MCPTT Server)?	-->	SIP 200 (OK)	3	P
23	Check: Does the IUT (MCPTT Server) send a SIP BYE message to the SS-UE2 (MCPTT client) to end the call via the participating server SS (MCPTT Server)?	-->	SIP BYE	3	P
24	The SS (MCPTT Server) responds with a SIP 200 (OK) message from SS-UE2 (MCPTT client)	<--	SIP 200 (OK)	-	-

7.1.3.3 Specific message contents

Table 7.1.3.3-1: SIP INVITE (Step 1, Table 7.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.5.2-1 condition MCPTT				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	The public service identity of the controlling MCPTT function		
From				
addr-spec				
user-info and host	px_MCPTT_Client_B_ID			
Session-Expires				
generic-param	any allowed value	The recommended initial value is 1800 in RFC 4028 [30].		
P-Asserted-Identity				
addr-spec				
user-info and host	px_MCX_SIP_PublicUserId_B_1			
Answer-Mode	not present			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP Message as described in Table 7.1.3.3-1A			
MIME body part		**MCPTT-INFO**		
MIME-part-body	MCPTT-Info as described in Table 7.1.3.3-2			
MIME body part		**Resource-Lists**		
MIME-part-body	Resource-lists as described in TS 36.579-1 [2], Table 5.5.3.3.2-1			

Table 7.1.3.3-1A: SDP in SIP INVITE (Table 7.1.3.3-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.2-1 condition SDP_OFFER, INITIAL_SDP_OFFER, IMPLICIT_GRANT_REQUESTED

Table 7.1.3.3-2: MCPTT-INFO in SIP INVITE (Table 7.1.3.3-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.1-1 conditions GROUP-CALL, INVITE_REFER				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
mcpttinfo				
mcptt-Params				
mcptt-calling-user-id	encrypted (NOTE 1) <mcptt-calling-user-id> with mcpttURI set to px_MCPTT_ID_User_B			
NOTE 1: Encrypted element as described in TS 36.579-1 [2] Table 5.5.3.2.1-1A				

Table 7.1.3.3-3: SIP INVITE (Step 3, Table 7.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.5.2-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_A	The public service identity of the terminating participating MCPTT function		
Contact				
addr-spec	SIP URI			
user-info and host	tsc_MCPTT_PublicServiceId_B			
Session-Expires				
generic-param	any allowed value	The recommended initial value is 1800 in RFC 4028 [30].		
P-Asserted-Identity				
addr-spec	tsc_MCPTT_PublicServiceId_B	The public service identity of the controlling MCPTT function		
Referred-By				
addr-spec	px_MCPTT_ID_User_B	Contains the public user identity of the inviting MCPTT user	TS 24.379 [9] clause 6.3.3.1.2	
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP Message as described in Table 7.1.3.3-3A			
MIME body part		**MCPTT-INFO**		
MIME-part-body	MCPTT-Info as described in Table 7.1.3.3-4			

Table 7.1.3.3-3A: SDP in SIP INVITE (Table 7.1.3.3-3)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.1-1 condition SDP_OFFER, INITIAL_SDP_OFFER

Table 7.1.3.3-4: MCPTT-INFO in SIP INVITE (Table 7.1.3.3-3)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.2-1 conditions GROUP-CALL

Table 7.1.3.3-5: SIP 183 (Session Progress) (Step 4, Table 7.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.16.3.2-1 conditions 100rel, MCPTT

Table 7.1.3.3-6: Void

Table 7.1.3.3-7: SIP 200 (OK) (Step 6, Table 7.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition INVITE-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec	tsc_MCPTT_PublicServiceId_B			
P-Answer-State				
value	"unconfirmed"			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP Message as described in Table 7.1.3.3-7A			

Table 7.1.3.3-7A: SDP in SIP 200 (OK) (Table 7.1.3.3-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.2-1 condition SDP_ANSWER, IMPLICIT_FLOOR_GRANTED, IMPLICIT_GRANT_REQUESTED

Table 7.1.3.3-8: SIP 200 (OK) (Step 7, Table 7.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition INVITE_RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 7.1.3.3-8A			
MIME body part		**MCPTT-Info**		
MIME-part-body	MCPTT-Info message as described in Table 7.1.3.3-8B			

Table 7.1.3.3-8A: SDP in SIP 200 (OK) (Table 7.1.3.3-8)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.1-1 condition SDP_ANSWER

Table 7.1.3.3-8B: MCPTT-Info in SIP 200 (OK) (Table 7.1.3.3-8)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.1-1 conditions GROUP-CALL, INVITE_RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
mcpttinfo				
mcptt-Params				
mcptt-calling-user-id	not present			
mcptt-called-party-id	encrypted <mcptt-called-party-id> with mcpttURI set to px_MCPTT_ID_User_A	Encrypted element as described in TS 36.579-1 [2] Table 5.5.3.2.1-1A		

Table 7.1.3.3-9: SIP 200 (OK) (Step 8, Table 7.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition INVITE_RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 7.1.3.3-9A			

Table 7.1.3.3-9A: SDP in SIP 200 (OK) (Table 7.1.3.3-9)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.2-1 conditions SDP_ANSWER, IMPLICIT_FLOOR_GRANTED, IMPLICIT_GRANT_REQUESTED

Table 7.1.3.3-10: Void

Table 7.1.3.3-11: Void

Table 7.1.3.3-12: SIP BYE (Step 21, Table 7.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.2.2-1 condition MT_CALL

Table 7.1.3.3-13: SIP BYE (Step 23, Table 7.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.2.1-1 condition MT_CALL

Table 7.1.3.3-14: Void

Table 7.1.3.3-15: Void

Table 7.1.3.3-16: Floor Taken (Step 11, Table 7.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.7-1 condition ON-NETWORK

Table 7.1.3.3-17: Floor Taken (Step 17, Table 7.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.7-1 condition ON-NETWORK			
Information Element	**Value/remark**	**Comment**	**Condition**
Granted Party's Identity			
Granted Party's Identity	px_MCPTT_User_A_ID		

Table 7.1.3.3-18: Floor Release (Steps 12, 18, Table 7.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.5-1 condition ON-NETWORK

Table 7.1.3.3-19: Void

Table 7.1.3.3-20: Void

Table 7.1.3.3-21: Floor Request (Step 15, Table 7.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.2-1 condition ON-NETWORK			
Information Element	**Value/remark**	**Comment**	**Condition**
Floor priority	"0"		

Table 7.1.3.3-22: Floor Granted (Step 16, Table 7.1.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.3-1 condition ON-NETWORK

7.2 MCPTT Server - MCPTT Server / On-demand Pre-arranged Group Call / Automatic Commencement Mode / Floor Control / Participating Server

7.2.1 Test Purpose (TP)

(1)

```
with { IUT (MCPTT Server) connected to PLMN1 }
ensure that {
  when { the SS-UE2 (MCPTT client) initiates registration }
    then { IUT (MCPTT Server) initially responds to the SS-UE2 (MCPTT client) with a SIP 401
Unauthorized message and continues the process by responding to the SS-UE2 (MCPTT client) with SIP
200 (OK) messages}
            }
```

(2)

```
with { IUT (MCPTT Server) connected to SS (MCPTT Server) and PLMN1 }
ensure that {
  when { the SS-UE2 (MCPTT client) initiates a pre-arranged group call with automatic commencement
mode }
    then { IUT (MCPTT Server) interacts with SS (MCPTT Server) and SS-UE2 (MCPTT client) to set up
the call by sending SIP messages }
            }
```

(3)

```
with { IUT (MCPTT Server) having established an MCPTT On-demand Pre-arranged Group Call with
Automatic Commencement Mode }
ensure that {
  when { the SS-UE1 (MCPTT client) and SS-UE2 (MCPTT client) engage in communication }
    then { IUT (MCPTT Server) forwards floor control messages to the controlling server SS (MCPTT
Server) and to the SS (MCCPT Client B) }
            }
```

(4)

```
with { IUT (MCPTT Server) having established an MCPTT On-demand Pre-arranged Group Call with
Automatic Commencement Mode }
ensure that {
  when { the SS (MCPTT Server) ends the pre-arranged group call }
    then { IUT (MCPTT Server) responds to the SS (MCPTT Server) by sending a SIP 200 (OK) message
and sends a SIP BYE message to the SS-UE2 (MCPTT client) }
            }
```

7.2.2 Conformance requirements

References: The conformance requirements covered in the present TC are specified in: TS 24.379 clause 10.1.1.3.1.1, 6.3.2.1.3, 6.3.2.2.4.2, 6.3.2.1.5.2, 6.3.2.2.8.1, TS 24.380 clause 6.4.2. Unless otherwise stated these are Rel-13 requirements.

[TS 24.379 clause 10.1.1.3.1.1]

In the procedures in this subclause:

1) group identity in an incoming SIP INVITE request refers to the group identity from the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request;

2) emergency indication in an incoming SIP INVITE request refers to the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

3) imminent peril indication in an incoming SIP INVITE request refers to the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body.

Upon receipt of a "SIP INVITE request for originating participating MCPTT function" containing an application/vnd.3gpp.mcptt-info+xml MIME body with the <session-type> element set to a value of "prearranged", the participating MCPTT function:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the SIP INVITE request with a SIP 500 (Server Internal Error) response. The participating MCPTT function may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [24]. Otherwise, continue with the rest of the steps;

NOTE 1: if the SIP INVITE request contains an emergency indication or an imminent peril indication set to a value of "true" and this is an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1, the participating MCPTT function can according to local policy choose to accept the request.

2) shall determine the MCPTT ID of the calling user from public user identity in the P-Asserted-Identity header field of the SIP INVITE request, and shall authorise the calling user;

NOTE 2: The MCPTT ID of the calling user is bound to the public user identity at the time of service authorisation, as documented in subclause 7.3.

3) if through local policy in the participating MCPTT function, the user identified by the MCPTT ID is not authorised to initiate prearranged group calls, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "109 user not authorised to make prearranged group calls" in a Warning header field as specified in subclause 4.4;

4) shall validate the media parameters and if the MCPTT speech codec is not offered in the SIP INVITE request shall reject the request with a SIP 488 (Not Acceptable Here) response. Otherwise, continue with the rest of the steps;

5) shall check if the number of maximum simultaneous MCPTT group calls supported for the MCPTT user as specified in the <MaxSimultaneousCallsN6> element of the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.384 [50]) has been exceeded. If exceeded, the participating MCPTT function shall respond with a SIP 486 (Busy Here) response with the warning text set to "103 maximum simultaneous MCPTT group calls reached" in a Warning header field as specified in subclause 4.4. Otherwise, continue with the rest of the steps;

NOTE 3: If the SIP INVITE request contains an emergency indication or an imminent peril indication, the participating MCPTT function can by means beyond the scope of this specification choose to allow for an exception to the limit for the maximum simultaneous MCPTT sessions supported for the MCPTT user. Alternatively, a lower priority session of the MCPTT user could be terminated to allow for the new session.

6) if the user identified by the MCPTT ID is not affiliated to the group identified in the "SIP INVITE request for originating participating MCPTT function" as determined by subclause 9.2.2.2.11 and this is an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1, shall perform the actions specified in subclause 9.2.2.2.12 for implicit affiliation;

7) if the actions for implicit affiliation specified in step 6) above were performed but not successful in affiliating the MCPTT user due to the MCPTT user already having N2 simultaneous affiliations, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 486 (Busy Here) response with the warning text set to "102 too many simultaneous affiliations" in a Warning header field as specified in subclause 4.4. and skip the rest of the steps.

NOTE 4: N2 is the total number of MCPTT groups that an MCPTT user can be affiliated to simultaneously as specified in 3GPP TS 23.179 [3].

NOTE 5: if the SIP INVITE request contains an emergency indication set to a value of "true" or an imminent peril indication set to a value of "true" and this is an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1, the participating MCPTT function can according to local policy choose to allow an exception to the N2 limit. Alternatively, a lower priority affiliation of the MCPTT user could be cancelled to allow for the new affiliation.

8) shall determine the public service identity of the controlling MCPTT function associated with the group identity in the SIP INVITE request;

NOTE 6: The public service identity can identify the controlling MCPTT function in the primary MCPTT system or a partner MCPTT system.

NOTE 7: How the participating MCPTT server discovers the public service identity of the controlling MCPTT function associated with the group identity is out of scope of the current release.

9) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.3;

10) shall set the Request-URI to the public service identity of the controlling MCPTT function associated with the group identity which was present in the incoming SIP INVITE request;

11) shall not copy the following header fields from the incoming SIP INVITE request to the outgoing SIP INVITE request, if they were present in the incoming SIP INVITE request:

   a) Answer-Mode header field as specified in IETF RFC 5373 [18]; and

   b) Priv-Answer-Mode header field as specified in IETF RFC 5373 [18];

12) shall set the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request to the MCPTT ID of the calling user;

13) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the MCPTT client as specified in subclause 6.3.2.1.1.1;

14) if the received SIP INVITE request contains an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in clause F.3 and if not already copied, shall copy the contents of the application/vnd.3gpp.mcptt-location-info+xml MIME body received in the SIP INVITE request into an application/vnd.3gpp.mcptt-location-info+xml MIME body included in the outgoing SIP request;

15) if a Resource-Priority header field was included in the received SIP INVITE request, shall include a Resource-Priority header field according to rules and procedures of 3GPP TS 24.229 [4] set to the value indicated in the Resource-Priority header field of the SIP INVITE request from the MCPTT client; and

NOTE 8: The participating MCPTT function will leave verification of the Resource-Priority header field to the controlling MCPTT function.

16) shall forward the SIP INVITE request, according to 3GPP TS 24.229 [4].

Upon receipt of a SIP 302 (Moved Temporarily) response to the above SIP INVITE request, the participating MCPTT function:

1) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.10;

2) shall include an SDP offer based upon the SDP offer in the received SIP INVITE request from the MCPTT client as specified in subclause 6.3.2.1.1.1; and

3) shall forward the SIP INVITE request according to 3GPP TS 24.229 [4].

Upon receipt of a SIP 2xx response in response to the above SIP INVITE request, the participating MCPTT function:

1) if the received SIP 2xx response contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <MKFC-GKTPs> element, shall perform the procedures in subclause 6.3.2.3.2;

2) shall generate a SIP 200 (OK) response as in subclause 6.3.2.1.5.2;

3) shall include in the SIP 200 (OK) response an SDP answer as specified in the subclause 6.3.2.1.2.1;

4) shall include Warning header field(s) that were received in the incoming SIP 200 (OK) response;

5) shall include the public service identity received in the P-Asserted-Identity header field of the incoming SIP 200 (OK) response into the P-Asserted-Identity header field of the outgoing SIP 200 (OK) response;

6) shall include an MCPTT session identity mapped to the MCPTT session identity provided in the Contact header field of the received SIP 200 (OK) response;

7) if the procedures of subclause 9.2.2.2.12 for implicit affiliation were performed in the present subclause, shall complete the implicit affiliation by performing the procedures of subclause 9.2.2.2.13;

8) shall send the SIP 200 (OK) response to the MCPTT client according to 3GPP TS 24.229 [4];

9) shall interact with Media Plane as specified in 3GPP TS 24.380 [5]; and

10) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [7].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request, the participating MCPTT function:

1) shall generate a SIP response according to 3GPP TS 24.229 [4];

2) shall include Warning header field(s) that were received in the incoming SIP response;

3) shall forward the SIP response to the MCPTT client according to 3GPP TS 24.229 [4]; and

4) if the implicit affiliation procedures of subclause 9.2.2.2.12 were invoked in this procedure, shall perform the procedures of subclause 9.2.2.2.14;

[TS 24.379 clause 6.3.2.1.3]

This subclause is referenced from other procedures.

When generating an initial SIP INVITE request according to 3GPP TS 24.229 [4], on receipt of an incoming SIP INVITE request, the participating MCPTT function:

1) shall include in the SIP INVITE request all Accept-Contact header fields and all Reject-Contact header fields, with their feature tags and their corresponding values along with parameters according to rules and procedures of IETF RFC 3841 [6] if included in the incoming SIP INVITE request;

2) should include the Session-Expires header field according to IETF RFC 4028 [7]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

3) shall include the option tag "timer" in the Supported header field;

4) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP INVITE request to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

5) shall include the g.3gpp.mcptt media feature tag into the Contact header field of the outgoing SIP INVITE request;

6) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [4]), into the P-Asserted-Service header field of the outgoing SIP INVITE request;

7) if the incoming SIP INVITE request contained a MIME resource-lists body with the MCPTT ID of the invited MCPTT user, shall copy the MIME resource-lists body, according to rules and procedures of IETF RFC 5366 [20];

8) if the incoming SIP INVITE request contained an application/vnd.3gpp.mcptt-info+xml MIME body, shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request to the outgoing SIP INVITE request; and

9) if the incoming SIP INVITE request contained an application/vnd.3gpp.mcptt-location-info+xml MIME body, shall copy the contents of the application/vnd.3gpp.mcptt-location-info+xml MIME body of the incoming SIP INVITE request to the outgoing SIP INVITE request.

[TS 24.379 clause 6.3.2.2.4.2]

This subclause is referenced from other procedures.

When sending SIP 200 (OK) responses, the participating MCPTT function shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [4] and:

1) shall include the option tag "timer" in a Require header field;

2) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [7], "UAS Behavior". If no "refresher" parameter was included in the SIP INVITE request, the "refresher" parameter in the Session-Expires header field shall be set to "uas";

3) shall include the following in the Contact header field:

   a) the g.3gpp.mcptt media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

   c) an MCPTT session identity mapped to the MCPTT session identity provided in the Contact header field of the received SIP INVITE request from the controlling MCPTT function;

4) shall include the option tag "tdialog" in a Supported header field according to rules and procedures of IETF RFC 4538 [23]; and

5) if the incoming SIP response contained an application/vnd.3gpp.mcptt-info+xml MIME body, shall copy the application/vnd.3gpp.mcptt-info+xml MIME body to the outgoing SIP 200 (OK) response.

[TS 24.379 clause 6.3.2.1.5.2]

This subclause is referenced from other procedures.

When sending SIP 200 (OK) responses, the participating MCPTT function shall generate a SIP 200 (OK) response according to 3GPP TS 24.229 [4] and:

1) shall include the option tag "timer" in a Require header field;

2) shall include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [7], "UAS Behavior". If the "refresher" parameter is not included in the received request, the "refresher" parameter in the Session-Expires header field shall be set to "uac";

3) shall include the following in the Contact header field:

   a) the g.3gpp.mcptt media feature tag;

   b) the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

   c) the isfocus media feature tag;

4) shall include the option tag "tdialog" in a Supported header field according to rules and procedures of IETF RFC 4538 [23];

5) shall include the option tag "norefersub" in a Supported header field according to rules and procedures of IETF RFC 4488 [22];

6) may include a Resource-Share header field in accordance with subclause 5.7.1.20.2 in 3GPP TS 24.229 [4]; and

7) if the incoming SIP 200 (OK) response contained an application/vnd.3gpp.mcptt-info+xml MIME body, shall copy the application/vnd.3gpp.mcptt-info+xml MIME body to the outgoing SIP 200 (OK) response.

[TS 24.379 clause 6.3.2.2.8.1]

Upon receiving a SIP BYE request from the controlling MCPTT function, the participating MCPTT function:

1) shall interact with the media plane as specified in subclause 6.4 in 3GPP TS 24.380 [5] for releasing media plane resource associated with the SIP session with the controlling MCPTT function;

2) shall generate a SIP BYE request according to 3GPP TS 24.229 [4];

3) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP BYE request to the P-Asserted-Identity header field of the outgoing SIP BYE request; and

4) shall send the SIP BYE request to the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the SIP BYE request the participating MCPTT function:

1) shall send a SIP 200 (OK) response to the SIP BYE request received from the controlling MCPTT function according to 3GPP TS 24.229 [4]; and

2) shall interact with the media plane as specified in 3GPP TS 24.380 [5] for releasing media plane resources associated with the SIP session with the MCPTT client.

[TS 24.380 clause 6.4.2]

Upon receiving a floor control message the participating MCPTT function:

1. shall immediately forward the floor control message to the floor control server if the message is received from the floor participant;

2. if an MBMS subchannel is not used for a conversation in the session the floor control message is associated with, shall immediately forward the floor control message to the floor participant if the message is received from the floor control server; and

3. if an MBMS subchannel is used for a conversation in the session the floor control message is associated with:

   a. if

      i. the floor control message is not a Floor Idle message or a Floor Taken message;

      ii. the MCPTT client has not reported "listening" status as specified in 3GPP TS 24.379 [2] subclause 14.2.3; or

      iii. the MCPTT client has reported "not-listening" status as specified in 3GPP TS 24.379 [2] subclause 14.2.3 in the latest received MBMS bearer listening status report;

      shall immediately forward the floor control message to the floor participant; and

   b. if

      i. the MCPTT client has reported "listening" status as specified in 3GPP TS 24.379 [2] subclause 14.2.3 in the latest received MBMS bearer listening status report; and

      ii if the floor control message is the Floor Idle message or the Floor Taken message,

   shall perform actions as specified in subclause 10.2.

NOTE: When the Floor Idle or Floor Taken messages are discarded the messages are sent to the MCPTT clients over the MBMS subchannel allocated for the conversation as specified in subclause 10.2.

7.2.3 Test description

7.2.3.1 Pre-test conditions

System Simulator:

- SS (MCPTT Server)

  - SS (MCPTT Server) provides the controlling MCPTT function and the terminating participating MCPTT function

- SS-UE1 (MCPTT client)
- SS-UE2 (MCPTT client)
- For the underlying "transport bearer" over which the SS-UE1 (MCPTT client) and SS-UE2 (MCPTT client) and the MCPTT Server will communicate, Parameters are set to the default parameters for the basic E-UTRA Single cell network scenarios, as defined in 3GPP TS 36.508 [22] clause 4.4. The simulated Cell 1 shall belong to PLMN1 (the PLMN specified for MCPTT operation in the MCPTT configuration document).

IUT:

- IUT (MCPTT Server)
  - IUT (MCPTT Server) provides the originating participating MCPTT function
- The IUT (MCPTT Server) consists of all sub-systems of the Common Services Core, including the Group Management Server, the Configuration Management Server, the Key Management Server, the Identity Management Server, the HTTP Server, and the SIP AS. The IUT (MCPTT Server) also consists of all sub-systems of the MCPTT Server, including the Media Distribution Function, the MCPTT User Database, the SIP AS, the HTPP Server, the HTTP Client, and the Floor Control Server.

Preamble:

- The IUT (MCPTT Server) is connected to SS (MCPTT Server) and to PLMN1 defined in TS 36.579-1 [2], Figure 4.2.6.
- SS-UE1 (MCPTT client) and SS-UE2 (MCPTT client) are affiliated with Group A and are authorized to initiate prearranged group calls
- Group A is controlled by the controlling MCPTT function, SS (MCPTT Server)

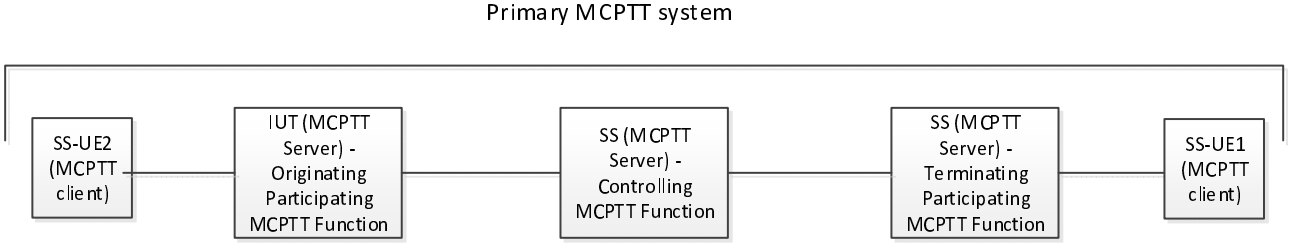

Figure 7.2.3.1-1: Functions of the testing components

7.2.3.2 Test procedure sequence

Table 7.2.3.2-1: Main behaviour

St	Procedure	Message Sequence		TP	Verdict
		U – S	Message		
-	EXCEPTION: In parallel to the event described in steps 1 to 4 below the SS-UE2 (MCPTT client) user authentication, authorization, and configuration as according to Table 5.1.3.2-1 takes place.	-	-	-	-
1	The SS-UE2 (MCPTT client) sends initial registration for IMS services	<--	SIP REGISTER	-	-
2	Check: Does the IUT (MCPTT Server) respond with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network?	-->	SIP 401 Unauthorized	1	P
3	The SS-UE2 (MCPTT client) completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials	<--	SIP REGISTER	-	-
4	Check: Does the IUT (MCPTT Server) send a SIP 200 (OK) to the SS-UE2 (MCPTT client)?	-->	SIP 200 OK	1	P
5-6	Void	-	-	-	-
7	The SS-UE2 (MCPTT client) sends a SIP INVITE message initiating a pre-arranged group call with automatic commencement mode	<--	SIP INVITE	-	-
8	Check: Does the IUT (MCPTT Server) send a SIP 100 (Trying) message to SS-UE2 (MCPTT client)?	-->	SIP 100 (Trying)	2	P
9	Check: Does the IUT (MCPTT Server) send a SIP INVITE message to the controlling server SS (MCPTT Server) for SS-UE1 (MCPTT client)?	-->	SIP INVITE	2	P
10	The SS (MCPTT Server) responds to the SIP INVITE message by sending a SIP 183 (Session Progress) message	<--	SIP 183 (Session Progress)	-	-
10A	Check: Does the IUT (MCPTT Server) send a SIP PRACK message to the server SS (MCPTT Server)?	-->	SIP PRACK	2	P
10B	The SS (MCPTT Server) responds to the SIP PRACK with a SIP 200 (OK) message.	<--	SIP 200 OK	-	-
10C	Check: Does the IUT (MCPTT Server) send a SIP 200 (OK) message to SS-UE2 (MCPTT Client) via the participating server SS (MCTT Server) with the P-Answer-State header field set to "unconfirmed"?	-->	SIP 200 (OK)	2	P
11	The SS (MCPTT Server) responds to the SIP INVITE message in step 9 by sending a SIP 200 (OK) message	<--	SIP 200 (OK)	-	-
-	EXCEPTION: In parallel to the events described in steps 12 to 13 the steps specified in Table 7.2.3.2-2 should take place.	-	-	-	-
12	Check: Does the IUT (MCPTT Server) respond to the SIP INVITE from the SS-UE2 (MCPTT client) sent in step 7 with a SIP 200 (OK) message?	-->	SIP 200 (OK)	2	P
13	The SS-UE2 (MCPTT client) responds with a SIP ACK message	<--	SIP ACK	-	-
14	Void	-	-	-	-
15	The SS-UE2 (MCPTT client) sends a Floor Release message with no acknowledgement required	<--	Floor Release	-	-
16	Check: Does the IUT (MCPTT Server) forward the Floor Release message to the SS (MCPTT Server)?	-->	Floor Release	3	P
17	The SS (MCPTT Server) sends a Floor Idle message to SS-UE2 (MCPTT client) via the IUT (MCPTT Server)	<--	Floor Idle	-	-

18	Check: Does the IUT (MCPTT Server) forward the Floor Idle message to the SS-UE2 (MCPTT client)?	-->	Floor Idle	3	P
19	The SS (MCPTT Server) sends a Floor Taken message to SS-UE2 (MCPTT client) via the IUT (MCPTT Server) informing that the floor has been taken by SS (MCPPT Client A)	<--	Floor Taken	-	-
20	Check: Does the IUT (MCPTT Server) forward the Floor Taken message to the SS-UE2 (MCPTT client)?	-->	Floor Taken	3	P
21	The SS (MCPTT Server) sends a Floor Idle message to SS-UE2 (MCPTT client) via the IUT (MCPTT Server)	<--	Floor Idle	-	-
22	Check: Does the IUT (MCPTT Server) forward the Floor Idle message to the SS-UE2 (MCPTT client)?	-->	Floor Idle	3	P
23	The SS (MCPTT Server) sends a SIP BYE request to SS-UE2 (MCPTT client) via the IUT (MCPTT Server)	<--	SIP BYE	-	-
24	Check: Does the IUT (MCPTT Server) send a SIP BYE message to the SS-UE2 (MCPTT client) to end the call?	-->	SIP BYE	4	P
25	The SS-UE2 (MCPTT client) responds with a SIP 200 (OK) message	<--	SIP 200 (OK)	-	-
26	Check: Does the IUT (MCPTT Server) send a SIP 200 (OK) message to SS (MCPTT Server)?	-->	SIP 200 (OK)	4	P

Table 7.2.3.2-2: Parallel Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	Check: Does the IUT (MCPTT Server) respond with a SIP ACK message to the controlling server SS (MCPTT Server)?	-->	SIP ACK	2	P

7.2.3.3 Specific message contents

Table 7.2.3.3-1: SIP REGISTER (Step 1, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.5.13-1 condition SIP_REGISTER_INITIAL				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	The public service identity of the MCPTT server under test		
From				
addr-spec				
user-info and host	px_MCX_SIP_PublicUserId_B_1			
AuthorizationTo				
username addr-spec	px_MCX_SIP_PrivateUserId_Bpx_MCPTT_Server_B_URI			

Table 7.2.3.3-2: Void

Table 7.2.3.3-2A: SIP REGISTER (Step 3, Table 6.1.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.13-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B	SIP URI of the home domain name		

Table 7.2.3.3-3: SIP 200 (OK) (Step 4, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition REGISTER-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
P-Associated-URI				
addr-spec[1]	SIP URI			
host	px_MCX_SIP_PublicUserId_B_1			

Table 7.2.3.3-3A: SIP 200 (OK) (Step 10C, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition INVITE-RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec	tsc_MCPTT_PublicServiceId_B			
P-Answer-State				
value	"unconfirmed"			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP Message as described in Table 7.2.3.3-3B			

Table 7.2.3.3-3B: SDP in SIP 200 (OK) (Table 7.2.3.3-3A)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.2-1 condition SDP_ANSWER, IMPLICIT_FLOOR_GRANTED, IMPLICIT_GRANT_REQUESTED

Table 7.2.3.3-4: SIP 200 (OK) (Step 11, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition INVITE_RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 7.2.3.3-4A			
MIME body part		**MCPTT-Info**		
MIME-part-body	MCPTT-Info message as described in Table 7.2.3.3-4B			

Table 7.2.3.3-4A: SDP in SIP 200 (OK) (Table 7.2.3.3-4)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.2-1 conditions SDP_ANSWER, IMPLICIT_GRANT_REQUESTED, IMPLICIT_FLOOR_GRANTED

Table 7.2.3.3-4B: MCPTT-Info in SIP 200 (OK) (Table 7.2.3.3-4)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.2-1 conditions GROUP-CALL				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
mcpttinfo				
mcptt-Params				
mcptt-calling-user-id	not present			
mcptt-called-party-id	encrypted <mcptt-called-party-id> with mcpttURI set to px_MCPTT_ID_User_A	Encrypted element as described in TS 36.579-1 [2] Table 5.5.3.2.1-1A		

Table 7.2.3.3-5: SIP 200 (OK) (Step 12, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.17.1.2-1 condition INVITE_RSP				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Contact				
addr-spec				
user-info and host	tsc_MCPTT_PublicServiceId_B			
Content-Type				
value	"multipart/mixed"			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 7.2.3.3-5A			
MIME body part		**MCPTT-Info**		
MIME-part-body	MCPTT-Info message as described in Table 7.2.3.3-4B			

Table 7.2.3.3-5A: SDP in SIP 200 (OK) (Table 7.2.3.3-5)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.2-1 conditions SDP_ANSWER, IMPLICIT_FLOOR_GRANTED, IMPLICIT_GRANT_REQUESTED

Table 7.2.3.3-6: Void

Table 7.2.3.3-7: Void

Table 7.2.3.3-8: SIP INVITE (Step 7, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.5.1-1 condition MCPTT				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_B			
From				
addr-spec				
user-info and host	Default public user id (px_MCX_SIP_PublicUserId_B_1)			
Session-Expires				
generic-param	"1800"	1800 seconds, or 30 minutes		
P-Asserted-Identity				
addr-spec	px_MCPTT_User_B_ID			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP message as described in Table 7.2.3.3-9			
MIME body part		**MCPTT-Info**		
MIME-part-body	MCPTT-Info message as described in Table 7.2.3.3-10			
MIME body part		**Resource-lists**		
MIME-part-body	Resource-lists message as described in Table 7.2.3.3-10A			

Table 7.2.3.3-9: SDP in SIP INVITE (Table 7.2.3.3-8)

TS 36.579-1 [2], Table 5.5.3.1.1-1 conditions SDP_OFFER, IMPLICIT_GRANT_REQUESTED

Table 7.2.3.3-10: MCPTT-Info in SIP INVITE (Table 7.2.3.3-8)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.1-1 condition GROUP-CALL, INVITE_REFER				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
mcpttinfo				
mcptt-Params				
mcptt-calling-user-id	encrypted (NOTE 1) <mcptt-calling-user-id> with mcpttURI set to px_MCPTT_ID_User_A			
NOTE 1: Encrypted element as described in TS 36.579-1 [2], Table 5.5.3.2.1-1A				

Table 7.2.3.3-10A: Resource-lists in SIP INVITE (Table 7.2.3.3-8)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.3.1-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
resource-lists	encrypted (NOTE 1)			
list[1]	encrypted (NOTE 1)			
name attribute	Not present			
display-name	Not present			
entry[1]	NOTE 4,5			
uri attribute	px_MCPTT_ID_User_A	The MCPTT ID of the invited user		
NOTE 1: XML encryption may be done by - element content encryption of the root element <resource-lists> as described in TS 36.579-1 [2], Table 5.5.13.2-1 - element content encryption of (each) <list> element as described in TS 36.579-1 [2], Table 5.5.13.2-1 - attribute URI encryption of the entry's uri attribute as described in TS 36.579-1 [2], Table 5.5.13.3-1				

Table 7.2.3.3-11: SIP INVITE (Step 9, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.5.1-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Request-URI	tsc_MCPTT_PublicServiceId_A	The public service identity of the controlling MCPTT function		
From				
addr-spec				
user-info and host	px_MCPTT_Client_B_ID			
Session-Expires				
generic-param	any allowed value	The recommended initial value is 1800 in RFC 4028 [30].		
P-Asserted-Identity				
addr-spec				
user-info and host	px_MCX_SIP_PublicUserId_B_1			
Answer-Mode	not present			
Message-body				
MIME body part		**SDP message**		
MIME-part-body	SDP Message as described in Table 7.2.3.3-11A			
MIME body part		**MCPTT-INFO**		
MIME-part-body	MCPTT-Info as described in Table 7.2.3.3-12			
MIME body part		**Resource-Lists**		
MIME-part-body	Resource-lists as described in Table 7.2.3.3-10A			

Table 7.2.3.3-11A: SDP in SIP INVITE (Table 7.2.3.3-11)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.1.1-1 condition SDP_OFFER, INITIAL_SDP_OFFER, IMPLICIT_GRANT_REQUESTED

Table 7.2.3.3-12: MCPTT-Info in SIP INVITE (Table 7.2.3.3-11)

Derivation Path: TS 36.579-1 [2], Table 5.5.3.2.1-1 condition GROUP-CALL				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
mcpttinfo				
mcptt-Params				
mcptt-calling-user-id	encrypted (NOTE 1) <mcptt-calling-user-id> with mcpttURI set to px_MCPTT_ID_User_B			

NOTE 1: Encrypted element as described in TS 36.579-1 [2] Table 5.5.3.2.1-1A

Table 7.2.3.3-12A: SIP 183 (Session Progress) (Step 10, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.16.3.2-1 conditions 100rel, MCPTT

Table 7.2.3.3-13: SIP BYE (Step 23, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.2.1-1 condition MT_CALL

Table 7.2.3.3-14: SIP BYE (Step 24, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.2-1 condition MT_CALL

Table 7.2.3.3-15: SIP ACK (Step 13, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.1.1-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Via				
sent-protocol	"SIP/2.0/UDP"			
sent-by	"sip:[5555::aaa:bbb:ccc :eed]"	SIP URI with IP address or FQDN and protected server port of UE		
	px_MCPTT_Client_B_ID":"protected server port as chosen by the UE			
via-branch	"z9hG4bKmcpttss33"			
Via				
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Server_A_ URI			
via-branch	"z9hG4bKmcpttss3"			
From				
addr-spec	px_MCPTT_Client_B_ URI			
To				
addr-spec	px_MCPTT_Server_A_ URI			

Table 7.2.3.3-16: SIP ACK (Step 14, Table 7.2.3.2-1)

Derivation Path: TS 36.579-1 [2], Table 5.5.2.1.2-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
From				
addr-spec	px_MCPTT_Server_B_URI			
To				
addr-spec	px_MCPTT_Server_A_URI			

Table 7.2.3.3-17: Floor Release (Steps 15, 16, Table 7.2.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.5-1 condition ON-NETWORK

Table 7.2.3.3-18: Void

Table 7.2.3.3-19: Floor Taken (Steps 19, 20, Table 7.2.3.2-1)

Derivation Path: 36.579-1 [2], Table 5.5.6.7-1 condition ON-NETWORK			
Information Element	**Value/remark**	**Comment**	**Condition**
Granted Party's Identity			
Granted Party's Identity	px_MCPTT_ID_User_A		

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-02	RAN5#74	R5-171300	-	-	-	Introduction of TS 36.579-3.	0.0.1
2018-03	RAN5#78	R5-180688	-	-	-	Incorporates changes agreed in: R5-181269 "New MCPTT Server TC 5.1" R5-181270 "New MCPTT Server TC 6.1" R5-181271 "New MCPTT Server TC 7.1" R5-181272 "New MCPTT Server TC 7.2"	0.1.0
2018-03	RAN#79	RP-180128	-	-	-	Draft version for information purposes to the RAN Plenary	1.0.0
2018-05	RAN5#79	R5-182438	-	-	-	Incorporates changes agreed in: R5-182421 R5-183162 R5-182486 R5-182487 R5-182488	2.0.0
2018-06	RAN#80	RP-180655	-	-	-	put under revision control as v13.0.0 with small editorial changes	13.0.0
2018-09	RAN#81	R5-192160	0001	-	F	Update 36.579-3 Typos in Forward and Section 4.1.2	13.1.0
2021-12	RAN#93	R5-217642	0002	-	F	Update of Test Case 5.1 - Authentication Authorization Configuration	13.2.0
2021-12	RAN#93	R5-217972	0003	1	F	Update of Test Case 6.1 - Client-Server Call	13.2.0
2021-12	RAN#93	R5-217973	0004	1	F	Update of Test Case 7.1 - Controlling Server Call	13.2.0
2021-12	RAN#93	R5-217974	0005	1	F	Update of Test Case 7.2 - Participating Server Call	13.2.0

History

Document history		
V13.0.0	July 2018	Publication
V13.1.0	May 2019	Publication
V13.2.0	January 2022	Publication