ETSI TS 124 379 V14.4.0 (2018-01)

LTE;
Mission Critical Push To Talk (MCPTT) call control;
Protocol specification
(3GPP TS 24.379 version 14.4.0 Release 14)

Reference
RTS/TSGC-0124379ve40

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

Intellectual Property Rights

Essential patents

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

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

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.

Foreword

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

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

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

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.

1 Scope

The present document specifies the session control protocols needed to support Mission Critical Push To Talk (MCPTT). The present document specifies both on-network and off-network protocols.

Mission critical communication services are services that require preferential handling compared to normal telecommunication services, e.g. in support of police or fire brigade.

The MCPTT service can be used for public safety applications and also for general commercial applications (e.g., utility companies and railways).

The present document is applicable to User Equipment (UE) supporting the MCPTT client functionality, and to application servers supporting the MCPTT server functionality.

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.*

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

[2] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT) over LTE; Stage 1".

[3] 3GPP TS 23.379: "Functional architecture and information flows to support mission critical communication services; Stage 2".

[4] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[5] 3GPP TS 24.380: "Mission Critical Push To Talk (MCPTT) floor control Protocol specification".

[6] IETF RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)".

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

[8] Void .

[9] IETF RFC 6050 (November 2010): "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[10] IETF RFC 3550 (July 2003): "RTP: A Transport Protocol for Real-Time Applications".

[11] Void.

[12] IETF RFC 4566 (July 2006): "Session Description Protocol".

[13] IETF RFC 3605 (October 2003): "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)".

[14] IETF RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[15] IETF RFC 5626 (October 2009): "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)".

[16] IETF RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

[17] IETF RFC 5245 (April 2010): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer Answer Protocols".

[18] IETF RFC 5373 (November 2008): "Requesting Answering Modes for the Session Initiation Protocol (SIP)".

[19] Void.

[20] IETF RFC 5366 (October 2008): "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)".

[21] IETF RFC 2046 (November 1996): "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[22] IETF RFC 4488 (May 2006): "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription".

[23] IETF RFC 4538 (June 2006): "Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)".

[24] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[25] IETF RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) Refer Method".

[26] IETF RFC 6665 (July 2012): "SIP-Specific Event Notification".

[27] IETF RFC 7647 (September 2015): "Clarifications for the use of REFER with RFC6665".

[28] 3GPP TS 24.334: "Proximity-services (ProSe) User Equipment (UE) to Proximity-services (ProSe) Function Protocol aspects; Stage 3".

[29] IETF RFC 4412 (February 2006): "Communications Resource Priority for the Session Initiation Protocol (SIP)".

[30] IETF RFC 4575 (August 2006): "A Session Initiation Protocol (SIP) Event Package for Conference State".

[31] 3GPP TS 24.481: "Mission Critical Services (MCS) group management Protocol specification".

[32] IETF RFC 4483 (May 2006): "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages.

[33] IETF RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[34] IETF RFC 4964 (October 2007): "The P-Answer-State Header Extension to the Session Initiation Protocol for the Open Mobile Alliance Push-to-talk over Cellular".

[35] IETF RFC 7614 (August 2015): "Explicit Subscriptions for the REFER Method".

[36] IETF RFC 5318 (December 2008): "The Session Initiation Protocol (SIP) P-Refused-URI-List Private-Header (P-Header)".

[37] IETF RFC 3903 (October 2004): "Session Initiation Protocol (SIP) Extension for Event State Publication".

[38] IETF RFC 5368 (October 2008): "Referring to Multiple Resources in the Session Initiation Protocol (SIP)".

[39] IETF RFC 5761 (April 2010): "Multiplexing RTP Data and Control Packets on a Single Port".

[40] 3GPP TS 23.003: "Numbering, addressing and identification".

[41] 3GPP TS 23.203: "Policy and charging control architecture".

[42] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference Point; Stage 3".

[43] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[44] IETF RFC 3264 (June 2002): "An Offer/Answer Model with the Session Description Protocol (SDP)".

[45] 3GPP TS 24.483: "Mission Critical Services (MCS) Management Object (MO)".

[46] Void.

[47] IETF RFC 4567 (July 2006): "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)".

[48] IETF RFC 8101 "IANA Registration of New Session Initiation Protocol (SIP) Resource-Priority Namespace for Mission Critical Push To Talk service".

[49] 3GPP TS 24.482: "Mission Critical Services (MCS) identity management Protocol specification.

[50] 3GPP TS 24.484: "Mission Critical Services (MCS) configuration management Protocol specification".

[51] IETF RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[52] IETF RFC 3863 (August 2004): "Presence Information Data Format (PIDF)".

[53] IETF RFC 7519 (May 2015): "JSON Web Token (JWT)".

[54] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[55] IETF RFC 4354 (January 2006): "A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service".

[56] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[57] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".

[58] 3GPP TS 24.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 3".

[59] 3GPP TS 29.199-9: "Open Service Access (OSA); Parlay X Web Services; Part 9: Terminal location".

[60] W3C: "XML Encryption Syntax and Processing Version 1.1", https://www.w3.org/TR/xmlenc-core1/.

[61] W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core/.

[62] IETF RFC 2392 (August 1998): "Content-ID and Message-ID Uniform Resource Locators".

[63] IETF RFC 4661 (September 2006): "An Extensible Markup Language (XML)-Based Format for Event Notification Filtering".

[64] IETF RFC 6086 (January 2011): "Session Initiation Protocol (SIP) INFO Method and Package Framework".

[65] IETF RFC 3891 (September 2004): "The Session Initiation Protocol (SIP) Replaces Header".

[66] 3GPP TS 24.216: "Communication continuity managed object".

[67] IETF RFC 4122 (July 2005): "A Universally Unique IDentifier (UUID) URN Namespace".

[68] IETF RFC 2045 (November 1996): "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[69] 3GPP TS 26.179: "Mission Critical Push To Talk (MCPTT) Codecs and media handling".

[70] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[71] IETF RFC 4648 (October 2006): "The Base16, Base32, and Base64 Data Encodings".

[72] IETF RFC 5627 (October 2009): "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)".

[73] 3GPP TS 29.283: "Diameter Data Management Applications".

[74] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[75] IETF RFC 6509 (February 2012): "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)".

[76] 3GPP TS 22.280: "Mission Critical Services Common Requirements (MCCoRe); Stage 1".

[77] IETF RFC 7462 (March 2015): "URNs for the Alert-Info Header Field of the Session Initiation Protocol (SIP)".

[78] 3GPP TS 33.180: "Security of the mission critical service".

[79] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

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].

An MCPTT user is affiliated to an MCPTT group: The MCPTT user is listed as a member of the MCPTT group in the MCPTT group document, the MCPTT server owning the MCPTT group has authorised the MCPTT user's interest in the MCPTT group and the MCPTT server serving the MCPTT user has authorised the MCPTT user's interest in the MCPTT group.

An MCPTT user is affiliated to an MCPTT group at an MCPTT client: The MCPTT user is affiliated to the MCPTT group, the MCPTT client has a registered IP address for an IMPU related to the MCPTT ID, and the MCPTT server serving the MCPTT user has authorised the MCPTT user's interest in the MCPTT group at the MCPTT client.

Affiliation status: Applies for an MCPTT user to an MCPTT group and has one of the following states:

a) the "not-affiliated" state indicating that the MCPTT user is not interested in the MCPTT group and the MCPTT user is not affiliated to the MCPTT group;

b) the "affiliating" state indicating that the MCPTT user is interested in the MCPTT group but the MCPTT user is not affiliated to the MCPTT group yet;

c) the "affiliated" state indicating that the MCPTT user is affiliated to the MCPTT group and there was no indication that MCPTT user is no longer interested in the MCPTT group; and

d) the "deaffiliating" state indicating that the MCPTT user is no longer interested in the MCPTT group but the MCPTT user is still affiliated to the MCPTT group.

Ambient listening call: a call type allowing an authorized MCPTT user to cause an MCPTT client to initiate a communication which results in no indication on the MCPTT UE that it is transmitting. Ambient listening can be initiated by an authorized MCPTT user who wants to be listened to by another authorized MCPTT user or can be initiated by an authorized MCPTT user who wants to listen to another MCPTT user.

Ambient listening client role: the role of an MCPTT client in an ambient listening call, which can be that of:

a) the "listening MCPTT user"; or

b) the "listened-to MCPTT user".

Ambient listening type: the type of an ambient listening call from the perspective of the relationship of the initiator of the call to the user being listened to. The two types of ambient listening call are:

a) "remote-init", indicating that the listening MCPTT user initiated the call; and

b) "local-init", indicating that the listened-to MCPTT user initiated the call.

First-to-answer call: A call initiated by one user towards a list of other users with the intention to establish an MCPTT private call or MCPTT emergency private call, with one of the users in the list of users.

Group identity: An MCPTT group identity or a temporary MCPTT group identity.

In-progress emergency private call state: the state of two participants when an MCPTT emergency private call is in progress.

In-progress imminent peril group state: the state of a group when an MCPTT imminent peril group call is in progress.

Listening MCPTT user: the MCPTT user in an ambient listening call receiving the media transmission from the listened-to MCPTT user;

Listened-to MCPTT user: the MCPTT user in an ambient listening call who is being listened to, may or may not be aware of being listened to depending on ambient listening type of the call.

MCPTT client ID: is a globally unique identification of a specific MCPTT client instance. MCPTT client ID is a UUID URN as specified in IETF RFC 4122 [67].

MCPTT emergency alert state: MCPTT client internal perspective of the state of an MCPTT emergency alert.

MCPTT emergency group state: MCPTT client internal perspective of the in-progress emergency state of an MCPTT group maintained by the controlling MCPTT function.

MCPTT emergency group call state: MCPTT client internal perspective of the state of an MCPTT emergency group call.

MCPTT emergency private call: MCPTT emergency call between two MCPTT users that is initiated as a private call or a first-to-answer call with emergency indication, or without emergency indication when the MCPTT emergency state is already set,

MCPTT emergency private call state: MCPTT client internal perspective of the state of an MCPTT emergency private call.

MCPTT emergency private priority state: MCPTT client internal perspective of the in-progress emergency private call state of the two participants of an MCPTT emergency private call maintained by the controlling MCPTT function.

MCPTT imminent peril group call state: MCPTT client internal perspective of the state of an MCPTT imminent peril group call.

MCPTT imminent peril group state: MCPTT client internal perspective of the state of an MCPTT imminent peril group.

MCPTT private call: MCPTT call between two MCPTT users that is initiated as a private call or a first-to-answer call.

MCPTT private emergency alert state: MCPTT client internal perspective of the state of an MCPTT private emergency alert targeted to an MCPTT user.

MCPTT speech: Conversational audio media used in mission critical push to talk systems as defined by 3GPP TS 22.179 [2] and 3GPP TS 23.379 [3].

Media-floor control entity: A media control resource shared by participants in an MCPTT session, controlled by a state machine to ensure that only one participant can access the media resource at the same time.

Private call: A call initiated by one user towards one other user with the intention to establish an MCPTT private call or MCPTT emergency private call.

Private Call Call-Back: A mechanism for a requesting MCPTT client to request a targeted MCPTT client to initiate an MCPTT private call with the requesting MCPTT client (at earliest convenience).

Remote change of an MCPTT user's selected group: A mechanism allowing an authorised user to remotely change the selected group of another MCPTT user.

Temporary MCPTT group identity: A group identity representing a temporary grouping of MCPTT group identities formed by the group regrouping operation as specified in 3GPP TS 24.481 [31].

Trusted mutual aid: A business relationship whereby the Partner MCPTT system is willing to share the details of the members of an MCPTT group that it owns with the Primary MCPTT system.

Untrusted mutual aid: A business relationship whereby the Partner MCPTT system is not willing to share the details of the members of an MCPTT group that it owns with the Primary MCPTT system.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.179 [2] 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 [5] apply:

MBMS subchannel

For the purpose of the present document, the following terms and definitions given in 3GPP TS 23.379 [3] apply:

Pre-selected MCPTT user profile
Selected MCPTT user profile

For the purpose of the present document, the following terms and definitions given in 3GPP TS 33.180 [78] apply:

Client Server Key (CSK)
Multicast Floor Control Key (MKFC)
Multicast Signalling Key (MuSiK)
Multicast Signalling Key Identifier (MuSiK-ID)
MBMS subchannel control key (MSCCK)
MBMS subchannel control key identifier (MSCCK-ID)
Private Call Key (PCK)
Signalling Protection Key (SPK)
XML Protection Key (XPK)

3.2 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].

CSK	Client-Server Key
ECGI	E-UTRAN Cell Global Identification
IPEG	In-Progress Emergency Group
IPEPC	In-Progress Emergency Private Call
IPIG	In-Progress Imminent peril Group
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
MC	Mission Critical

MCS	Mission Critical Service
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
PCC	Policy and Charging Control
PCCB	Private Call Call-Back
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
SPK	Signalling Protection Key
SSRC	Synchronization SouRCe
TGI	Temporary MCPTT Group Identity
TMGI	Temporary Mobile Group Identity
UE	User Equipment
URI	Uniform Resource Identifier
XPK	XML Protection Key

4 General

4.1 MCPTT overview

The MCPTT service supports communication between several users (i.e. group call), where each user has the ability to gain access to the permission to talk in an arbitrated manner. The MCPTT service also supports private calls between two users. Group calls and private calls can be provided on-network and off-network. In this release of the present document, support is only allowed for MCPTT speech communications.

The present document provides the call control protocol enhancements to support the MCPTT architectural procedures specified in 3GPP TS 23.379 [3].

For on-network calls, the present document makes use of the existing IMS procedures specified in 3GPP TS 24.229 [4], and provides new IMS application procedures specific for MCPTT. For on-network group calls, the procedures in the present document allow the use of unicast or multicast bearers.

The on-network procedures in this document allow an MCPTT user to:

- initiate a new MCPTT group session;
- join an MCPTT group session that has already been established; and
- leave an established MCPTT group session and then re-join the same MCPTT group session if still established.

For off-network calls, the present document utilises the procedures for ProSe direct discovery for public safety and the procedures for one-to-one ProSe direct communication for Public Safety, as specified in 3GPP TS 24.334 [28]. The present document specifies the MCPTT Off-Network Protocol (MONP) and the MONP application procedures.

For on-network and off-network calls, the present document provides support for MCPTT emergency calls, MCPTT imminent-peril calls and MCPTT emergency alerts.

NOTE: MCPTT emergency calls do not utilise emergency bearers. Instead the EPS bearer priority of a normal bearer is adjusted.

The MCPTT procedures provided by the present document refer to:

- the floor-control procedures defined in 3GPP TS 24.380[5];
- the group management procedures defined in 3GPP TS 24.481 [31];
- the identity management procedures defined in 3GPP TS 24.482 [49];
- the security procedures defined in 3GPP TS 33.180 [78]; and
- the PS-PS access transfer procedures procedures defined in 3GPP TS 24.237 [58].

The MCPTT procedures provided by the present document access the configuration parameters provided by 3GPP TS 24.483 [45] and 3GPP TS 24.484 [50].

Codecs and media handling for MCPTT are specified in 3GPP TS 26.179 [69];

The following procedures are provided within this document:

- common procedures are specified in clause 6;
- procedures for registration in the IM CN subsystem and service authorisation are specified in clause 7;
- procedures for pre-established session establishment, modification and release are specified in clause 8;
- procedures for affiliation are specified in clause 9;
- procedures for on-network and off-network group call are specified in clause 10;
- procedures for on-network and off-network private call are specified in clause 11;
- procedures for on-network and off-network emergency alert are specified in clause 12;
- location procedures are specified in clause 13;
- MBMS transmission usage procedures are specified in clause 14; and
- MCPTT service continuity procedures are specified in clause 14A.

The MCPTT UE primarily obtains access to the MCPTT service via E-UTRAN, using the procedures defined in 3GPP TS 24.301 [70].

4.2 URI and address assignments

In order to support MCPTT, the following URI and address assignments are assumed:

1) the participating MCPTT function is configured to be reachable using:
   a) the public service identity identifying the pre-established session on the MCPTT server serving the MCPTT user;
   b) the MBMS public service identity of the participating MCPTT function; and
   c) the public service identity of the participating MCPTT function serving the MCPTT user.

NOTE: The above PSI values are configured with the same URI. However, in the present document the above names on the URIs are used for the purpose of readability.

4.3 MCPTT speech

A session that contains MCPTT speech is either a full-duplex session or a half-duplex session with an SDP media component containing an audio media type with a codec suitable for conversational speech that exists between an MCPTT client and an MCPTT server.

If the MCPTT speech session is a half-duplex session, it additionally contains a media component that describes the characteristics of the media-floor control entity.

4.4 Warning Header Field

4.4.1 General

The MCPTT server can include a free text string in a SIP response to a SIP request. When the MCPTT server includes a text string in a response to a SIP INVITE request the text string is included in a Warning header field as specified in IETF RFC 3261 [24]. The MCPTT server includes the Warning code set to 399 (miscellaneous warning) and includes the host name set to the host name of the MCPTT server.

EXAMPLE: Warning: 399 "100 User not authorised to make group calls"

4.4.2 Warning texts

The text string included in a Warning header field consists of an explanatory text preceded by a 3-digit text code, according to the following format in Table 4.4.2-1.

Table 4.4.2-1 ABNF for the Warning text

```
warn-text      =/  DQUOTE mcptt-warn-code SP mcptt-warn-text DQUOTE
mcptt-warn-code = DIGIT DIGIT DIGIT
mcptt-warn-text = *( qdtext | quoted-pair )
```

Table 4.4.2-2 defines the warning texts that are defined for the Warning header field when a Warning header field is included in a response to a SIP INVITE request as specified in subclause 4.4.1.

Table 4.4.2-2: Warning texts defined for the Warning header field

Code	Explanatory text	Description
100	function not allowed due to <detailed reason>	The function is not allowed to this user. The <detailed reason> will be either "group definition", "access policy", "local policy", "user authorisation" or “pre-established session not supported”, or can be a free text string.
101	service authorisation failed	The service authorisation of the MCPTT ID against the IMPU failed at the MCPTT server.
102	too many simultaneous affiliations	The MCPTT user already has N2 maximum number of simultaneous affiliations.
103	maximum simultaneous MCPTT group calls reached	The number of maximum simultaneous MCPTT group calls supported for the MCPTT user has been exceeded.
104	isfocus not assigned	A controlling MCPTT function has not been assigned to the MCPTT session.
105	subscription not allowed in a broadcast group call	Subscription to the conference event package rejected during a group call initiated as a broadcast group call.
106	user not authorised to join chat group	The MCPTT user is not authorised to join this chat group.
107	user not authorised to make private calls	The MCPTT user is not authorised to make private calls.
108	user not authorised to make chat group calls	The MCPTT user is not authorised to make chat group calls.
109	user not authorised to make prearranged group calls	The MCPTT user is not authorised to make group calls to a prearranged group.
110	user declined the call invitation	The MCPTT user declined to accept the call.
111	group call proceeded without all required group members	The required members of the group did not respond within the acknowledged call time, but the call still went ahead.
112	group call abandoned due to required group members not part of the group session	The group call was abandoned, as the required members of the group did not respond within the acknowledged call time.
113	group document does not exist	The group document requested from the group management server does not exist.
114	unable to retrieve group document	The group document exists on the group management server but the MCPTT server was unable to retrieve it.
115	group is disabled	The group has the <disabled> element set to "true" in the group management server.
116	user is not part of the MCPTT group	The group exists on the group management server but the requesting user is not part of this group.
117	the group identity indicated in the request is a prearranged group	The group id that is indicated in the request is for a prearranged group, but did not match the request from the MCPTT user.
118	the group identity indicated in the request is a chat group	The group id that is indicated in the request is for a chat group, but did not match the request from the MCPTT user.
119	user is not authorised to initiate the group call	The MCPTT user identified by the MCPTT ID is not authorised to initiate the group call.
120	user is not affiliated to this group	The MCPTT user is not affiliated to the group.
121	user is not authorised to join the group call	The MCPTT user identified by the MCPTT ID is not authorised to join the group call.
122	too many participants	The group call has reached its maximum number of participants.
123	MCPTT session already exists	Inform the MCPTT user that the group call is currently ongoing.
124	maximum number of private calls reached	The maximum number of private calls allowed at the MCPTT server for the MCPTT user has been reached.

125	user not authorised to make private call with automatic commencement	The MCPTT user is not authorised to make a private call with automatic commencement.
126	user not authorised to make private call with manual commencement	The MCPTT user is not authorised to make a private call with manual commencement.
127	user not authorised to be called in private call	The called MCPTT user is not allowed to be part of a private call.
128	isfocus already assigned	The MCPTT server owning an MCPTT group received a SIP INVITE request destined to the MCPTT group from another MCPTT server already assigned as the controlling MCPTT function and the MCPTT server owning the MCPTT group does not support mutual aid or supports trusted mutual aid but does not authorise trusted mutual aid.
136	authentication of the MIKEY-SAKKE I_MESSAGE failed	The MCPTT client's application of the procedures of 3GPP TS 33.180 [78] to authenticate the received I_MESSAGE fails.
137	the indicated group call does not exist	The participating MCPTT function cannot find an ongoing group session associated with the received MCPTT session identity.
138	subscription of conference events not allowed	The controlling MCPTT function could not allow the MCPTT user to subscribe to the conference event package.
139	integrity protection check failed	The integrity protection of an XML MIME body failed.
140	unable to decrypt XML content	The XML content cannot be decrypted.
141	user unknown to the participating function	The participating function is unable to associate the public user identity with an MCPTT ID.
142	unable to determine the controlling function	The participating function is unable to determine the controlling function for the group call or private call.
143	not authorised to force auto answer	The calling user is not authorised to force auto answer on the called user.
144	user not authorised to call this particular user	The calling user is not authorised to call this particular called user.
145	unable to determine called party	The participating function was unable to determine the called party from the information received in the SIP request.
146	T-PF unable to determine the service settings for the called user	The service settings have not been uploaded by the terminating client to the terminating participating server.
147	user is authorized to initiate a temporary group call	The non-controlling MCPTT function has authorized a request from the controlling MCPTT function to authorize a user to initiate an temporary group session.
148	MCPTT group is regrouped	The MCPTT group hosted by a non-controlling MCPTT function is part of a temporary group session as the result of the group regroup function.
149	SIP-INFO request pending	The MCPTT client needs to wait for a SIP-INFO request with specific content, before taking further action.
150	invalid combinations of data received in MIME body	The MCPTT client included invalid combinations of data in the SIP request.
151	user not authorised to make a private call call-back request	The MCPTT user is not authorised to make a private call call-back request.
152	user not authorised to make a private call call-back cancel request	The MCPTT user is not authorised to make a private call call-back cancel request.
153	user not authorised to call any of the users requested in the first-to-answer call	All users that were invited in the first-to-answer call cannot be involved in a private call with the inviting user.
154	user not authorised to make ambient listening call	The MCPTT user is not authorised to make an ambient listening call.

155	user not authorised to change user's selected group	The MCPTT user is not authorised to change the selected group of the targeted user.
156	user not authorised to originate a first-to-answer call	The MCPTT user is not authorised to make a first-to-answer call.

4.5 MCPTT session identity

The MCPTT session identity is a SIP URI, which identifies the MCPTT session between:

- the MCPTT client and the participating MCPTT function;
- the participating MCPTT function and the controlling MCPTT function
- the controlling MCPTT function and the non-controlling MCPTT function; and
- the non-controlling MCPTT function and the participating MCPTT function.

The MCPTT session identity shall be a GRUU as defined in IETF RFC 5627 [72] assigned by the MCPTT server as per 3GPP TS 24.229 [4].

The MCPTT session identity identifies the MCPTT session in such a way that e.g.:

- the MCPTT user is able to subscribe to the participant information of the ongoing MCPTT session;
- the MCPTT user is able to re-join an ongoing MCPTT session; and
- the IM CN subsystem is able to route an initial SIP request to the controlling MCPTT function.

The controlling MCPTT function allocates a unique MCPTT session identity hosted at the controlling MCPTT function for the MCPTT session at the time of session establishment.

The non-controlling MCPTT function allocates a unique MCPTT session identity hosted at the non-controlling MCPTT function for the MCPTT session at the time of session establishment.

When protection of sensitive application data is required by the MCPTT operator, the MCPTT session identity cannot contain identity information that is classed as sensitive such as the MCPTT ID or the MCPTT Group ID, as specified in subclause 4.8.

The controlling MCPTT function and non-controlling MCPTT function send the MCPTT session identity towards the MCPTT client during MCPTT session establishment by including it in the Contact header field of the final SIP response to a session initiation request.

The participating MCPTT function allocates a unique MCPTT session identity hosted at the participating MCPTT function for the MCPTT session when it receives a MCPTT session identity in the Contact header field of a SIP request or a SIP response from the controlling MCPTT function or non-controlling MCPTT function and includes it in the Contact header field of the SIP request or SIP response sent towards the MCPTT client. The participating MCPTT function maintains a mapping of the MCPTT session identities it sends to the MCPTT client to the corresponding MCPTT session identities received from the controlling MCPTT function.

The MCPTT client can cache the MCPTT session identity until a time when it is no longer needed.

The MCPTT session identity is also used in floor control requests and responses as specified in 3GPP TS 24.380 [5].

4.6 MCPTT priority calls and alerts

4.6.1 MCPTT emergency group calls

MCPTT emergency group calls as defined by 3GPP TS 23.379 [3] are supported by the procedures in this specification. The following MCPTT emergency group call functionalities are described:

- MCPTT emergency group call origination;

- upgrade of an MCPTT group call to an MCPTT emergency group call; and
- in-progress group emergency cancel.

NOTE 1: In-progress group emergency cancel means the cancellation of the in-progress emergency state of the group, which is managed by the controlling MCPTT function.

The above functionalities are supported using both MCPTT prearranged group calls and MCPTT chat group calls.

Key aspects of MCPTT emergency group calls include:

- adjusted EPS bearer priority for all participants whether or not they themselves are in an emergency condition (i.e. have their MCPTT emergency state set). For unicast bearers this is achieved by using the Resource-Priority header field as specified in IETF RFC 4412 [29] with namespaces defined for use by MCPTT specified in IETF RFC 8101 [48], and for MBMS bearers this is achieved by having the participating MCPTT function adjust the ARP (priority, PVI, PCI) and executing the Modify MBMS Bearer Procedure per 3GPP TS 29.468 [42];
- pre-emptive floor control priority over MCPTT users in MCPTT emergency group calls who themselves do not have their MCPTT emergency state set;
- restoration of normal EPS bearer priority to the call participants when the in-progress emergency group state is cancelled;
- restoration of normal floor control priority participants when the in-progress emergency group state is cancelled;
- requires the MCPTT user to be authorised to either originate or cancel an MCPTT emergency group call;
- requests to originate MCPTT emergency group calls may also include an indication of an MCPTT emergency alert; and
- requests to cancel MCPTT emergency group calls may also include an indication of cancelling a previously issued MCPTT emergency alert.

There are a number of states that are key in managing these aspects of MCPTT emergency group calls, which include:

- **MCPTT emergency state:** as defined in 3GPP TS 22.179 [2] and 3GPP TS 23.379 [3], indicates that the MCPTT user is in a life-threatening situation. Managed by the MCPTT user of the device or an authorised MCPTT user. While the MCPTT emergency state is set on the client, all calls originated by the client will be MCPTT emergency calls, assuming the MCPTT user is authorised for MCPTT emergency calls on them.
- **in-progress emergency group state:** as defined in 3GPP TS 22.179 [2] and 3GPP TS 23.379 [3], indicates whether or not there is an MCPTT emergency group call ongoing on the specified group. This state is managed by the controlling MCPTT function. All group calls originated on this MCPTT group when in an in-progress emergency state are MCPTT emergency group calls until this state is cancelled, whether or not the originator is themselves in an MCPTT emergency state.
- **MCPTT emergency group (MEG) state:** this is an internal state managed by the MCPTT client which tracks the in-progress emergency state of the group as defined in 3GPP TS 22.179 [2] and 3GPP TS 23.379 [3] and managed by the controlling MCPTT function. Ideally, the MCPTT client would not need to track the in-progress emergency group state, but doing so enables the MCPTT client to request MCPTT emergency-level priority earlier than otherwise possible. For example, if the MCPTT user wishes to join an MCPTT emergency group call and is not in MCPTT emergency state itself, the MCPTT client should have emergency level priority. If it has knowledge of the in-progress emergency state of the group, it can request priority by including a Resource-Priority header field set to the MCPTT namespace specified in IETF RFC 8101 [48], and appropriate priority level in the SIP INVITE request (or SIP re-INVITE request).
- **MCPTT emergency group call (MEGC) state**: this is an internal state managed by the MCPTT client which in conjunction with the MCPTT emergency alert state aids in managing the MCPTT emergency state and related actions.
- **MCPTT emergency alert (MEA) state**: this is also an internal state of the MCPTT client which in conjunction with the MCPTT emergency group call state aids in managing the MCPTT emergency state and related actions.

NOTE 2: The above states and their transitions are described in Annex G.

4.6.2 MCPTT emergency private calls

MCPTT emergency private calls as defined by 3GPP TS 23.379 [3] are supported by the procedures in this specification. The following MCPTT emergency private call functionalities are specified in the present document:

- MCPTT emergency private call origination with optional MCPTT emergency alert initiation;
- upgrade of an MCPTT private call to an MCPTT emergency private; and
- cancellation of the MCPTT emergency private call priority.

Key aspects of MCPTT emergency private calls include:

- adjusted EPS bearer priority for both participants whether or not they are both in an emergency condition (i.e. both have their MCPTT emergency state set). This is achieved by using the Resource-Priority header field as specified in IETF RFC 4412 [29] with namespaces defined for use by MCPTT specified in IETF RFC 8101 [48];
- the initiator of the MCPTT emergency private call can override the other MCPTT user in the MCPTT emergency private call unless that user also has their MCPTT emergency state set;
- restoration of normal EPS bearer priority to the call according to system policy (e.g., configured time limit for the emergency priority of an MCPTT emergency private call or cancellation of the emergency condition of the private call);
- restoration of normal floor control priority participants when the emergency elevated priority is cancelled;
- requires the MCPTT user to be authorised to either originate or cancel an MCPTT emergency private call;
- requires the targeted MCPTT user to be authorised to receive an MCPTT emergency private call;
- requests to originate MCPTT emergency private calls may also include an indication of an MCPTT emergency alert; and
- the originator of the MCPTT emergency private call can request that the call use either manaual or automatic commencement mode.

There are a number of states that are key in managing these aspects of MCPTT emergency private calls, which include:

- **MCPTT emergency state (MES):** as defined in 3GPP TS 22.179 [2] and 3GPP TS 23.379 [3], indicates that the MCPTT user is in a life-threatening situation. Managed by the MCPTT user of the device or an authorised MCPTT user. While the MCPTT emergency state is set on the client, all MCPTT group and private calls originated by the client will be MCPTT emergency calls, assuming the MCPTT user is authorised for MCPTT emergency calls on them.
- **MCPTT private emergency alert (MPEA) state**: this is an internal state of the MCPTT client which in conjunction with the MCPTT emergency private call state aids in managing the MCPTT emergency state and related actions.
- **MCPTT emergency private call (MEPC) state**: this is an internal state managed by the MCPTT client which in conjunction with the MCPTT emergency alert state aids in managing the MCPTT emergency state and related actions.
- **In-progress emergency private call (IPEPC) state:** indicates whether or not there is an MCPTT emergency private call in-progress for the two participants. This state is managed by the controlling MCPTT function. All private calls originated between these two participants when in an in-progress emergency private call state are MCPTT emergency private calls until this state is cancelled, whether or not the originator is in an MCPTT emergency state.
- **MCPTT emergency private priority (MEPP) state:** this is an internal state managed by the MCPTT client which tracks the in-progress emergency private call state of the private call managed by the controlling MCPTT function. Ideally, the MCPTT client would not need to track the in-progress emergency private priority state, but doing so enables the MCPTT client to request MCPTT emergency-level priority earlier than otherwise possible. For example, if the MCPTT user wishes to join an MCPTT emergency private call and is not in the MCPTT emergency state, the MCPTT client should have emergency level priority. If it has knowledge of the in-progress emergency private priority state of the private call (i.e., the two participants), it can request priority by including

a Resource-Priority header field set to the MCPTT namespace specified in IETF RFC 8101 [48], and appropriate priority level in the SIP INVITE request (or SIP re-INVITE request).

NOTE: The above states and their transitions are described in Annex G.

4.6.3 MCPTT emergency alerts

MCPTT emergency alerts as defined by 3GPP TS 23.379 [3] are supported by the procedures in this specification. The following MCPTT emergency group call functionalities are specified in the present document:

- MCPTT emergency alert origination; and
- MCPTT emergency alert cancellation.

MCPTT emergency alerts are supported procedurally by two general mechanisms. One mechanism is embedded within the MCPTT emergency call (both emergency private call and emergency group call using both prearranged and chat session models) signalling procedures documented in clause 10 and clause 11 of this specification. The other mechanism utilizes SIP MESSAGE requests and is documented in clause 12.

MCPTT emergency alerts can be initiated or cancelled as options in the following signalling procedures documented in clause 10 and clause 11:

- MCPTT emergency group call initiation;
- MCPTT group call upgraded to MCPTT emergency call;
- MCPTT emergency group call cancellation (i.e., in-progress emergency state of the group set to false);
- MCPTT emergency private call initiation; and
- MCPTT private call upgrade to MCPTT emergency private call.

MCPTT emergency alerts can also be initiated or cancelled as described in the procedures of clause 12 which include:

- MCPTT emergency alert initiation; and
- MCPTT emergency alert cancellation (with optional cancelling of the in-progress emergency state of a group).

When MCPTT emergency alerts are initiated as an option in initiating or upgrading to an MCPTT emergency group call or are initiated using SIP MESSAGE requests, they are targeted to an MCPTT group, and, if not already affiliated, will result in the initiator being implicitly affiliated to the MCPTT group. When initiated as an option in initiating or upgrading to an MCPTT emergency private call, an MCPTT emergency alert is targeted to an individual MCPTT user, not to an MCPTT group.

Key aspects of MCPTT emergency alerts include:

- **MCPTT emergency (MES) state:** the MCPTT client's MCPTT emergency state as described in clause G.1 is set upon initiation of an MCPTT emergency alert. While the MCPTT emergency state is set, assuming the MCPTT user has the needed authorisations, if the user initiates a private call and is authorised to do so, the MCPTT private call will be an MCPTT emergency private call. Similarly, assuming the needed authorisations, any subsequent MCPTT group call initiated by an MCPTT user with the MCPTT emergency state set will be an MCPTT emergency group call.
- **MCPTT emergency alert (MEA) state:** the MCPTT client maintains the internal MCPTT emergency alert state (MEA) which aids in the management of the MCPTT emergency state as described in clause G.5.
- **MCPTT private emergency alert (MPEA) state**: the MCPTT client maintains the MCPTT private emergency alert state of an MCPTT emergency alert targeted to an MCPTT user which aids in the management of the MCPTT emergency state.
- **In-progress emergency group (IPEG) state :** MCPTT emergency alert initiation or cancellation in and of itself does not impact the in-progress emergency state of the targeted group, which is maintained by the controlling MCPTT function, nor does it impact the priority of the EPS bearers. However, in setting the MCPTT emergency state, assuming an MCPTT user is authorised to make MCPTT emergency calls on the targeted group, any subsequent MCPTT group call the MCPTT user initiates on the group will cause the in-progress emergency state

of the group to be set as described in clause G.2 and will result in upgraded priority of the EPS bearers used in the MCPTT emergency call.

- **Authorisations for emergency alerts:** MCPTT users need to be authorised to initiate MCPTT emergency alerts and additionally need to be authorised to cancel MCPTT emergency alerts. The parameters related to these authorisations are specified in 3GPP TS 24.483 [45] and 3GPP TS 24.484 [50].

4.6.4 MCPTT imminent peril group call

MCPTT imminent peril group calls as defined by 3GPP TS 23.379 [3] are supported by the procedures in this specification. The following MCPTT imminent peril group calls functionalities are specified in the present document:

- MCPTT imminent peril group calls origination;
- upgrade of an MCPTT group call to an MCPTT imminent peril group call;
- upgrade from an MCPTT imminent peril group call to an MCPTT emergency group call; and
- cancellation of the in-progress imminent peril state of the group.

Key aspects of MCPTT imminent peril include:

- adjusted EPS bearer priority for all participants when the in-progress imminent peril state of the group is set whether or not they themselves initiated an imminent peril group call. For unicast bearers this is achieved by using the Resource-Priority header field as specified in IETF RFC 4412 [29] with namespaces defined for use by MCPTT specified in IETF RFC 8101 [48], and for MBMS bearers this is achieved by having the participating MCPTT function adjust the ARP (priority, PVI, PCI) and executing the Modify MBMS Bearer Procedure per 3GPP TS 29.468 [42];
- restoration of normal EPS bearer priority to the call when the in-progress imminent peril group state is cancelled; and
- requires the MCPTT user to be authorised to either originate or cancel an MCPTT imminent peril group call.

Relationship to other MCPTT priority group call types:

- A normal MCPTT group call can be upgraded to an MCPTT imminent peril group call;
- An MCPTT imminent peril group call can be upgraded to an MCPTT emergency group call;
- When either an MCPTT imminent peril group call or an MCPTT emergency group call (i.e., their respective "in-progress" states) the group call returns to the priority designated for normal group calls, i.e., their is no direct transition from an MCPTT emergency group call to an MCPTT imminent peril group call;
- MCPTT imminent peril functionality is only applicable to MCPTT group calls, not MCPTT private calls; and
- MCPTT imminent peril group calls have no associated alert capabilities such as the MCPTT emergency alert capability which is associated with MCPTT emergency group calls.

There are a number of states that are key in managing these aspects of MCPTT imminent peril group calls, which include:

- **MCPTT imminent peril group (MIG) state**: this is an internal state of the MCPTT client which in conjunction with the MCPTT imminent peril group call state aids the client in managing the use of the Resource-Priority header field and related actions.
- **MCPTT imminent peril group call (MIGC) state**: this is an internal state managed by the MCPTT client which in conjunction with the MCPTT imminent peril group state aids the client in managing the use of the Resource-Priority header field and related actions.
- **In-progress imminent peril group (IPIG) state:** this a state of the MCPTT group which is managed by the controlling MCPTT function. While an MCPTT group is in an in-progress imminent peril group state, all participants in group calls using this group will receive elevated priority.

The above states and their transitions are described in Annex G.

4.7 Communication security

4.7.1 Media security

If a mission critical organisation requires MCPTT users to communicate using end-to-end security, a security context needs to be established between the initiator of the call and the recipient(s) of the call, prior to the establishment of media, or floor control signalling. This provides assurance to MCPTT users that no unauthorised access to communications is taking place within the MCPTT network. An MCPTT key management server (KMS) manages the security domain. For any end-point to use or access end-to-end secure communications, it needs to be provisioned with keying material associated to its identity by the KMS as specified in 3GPP TS 33.180 [78].

For group calls, the security context is set up at the time of creation of the group or temporary group. The group management server creates group call keying material associated with the group and distributes it to all members of the group or temporary group, in advance of the initiation of a group call as specified in 3GPP TS 24.481 [31] and 3GPP TS 33.180 [78]. The establishment of a security context for group calls has no impact on this specification.

For private calls, the security context is initiated at call setup. An end-to-end security context is established that is unique to the pair of users involved in the call. The procedure involves transferral of an encapsulated private call key (PCK) and private call key id (PCK-ID) from the initiator to the terminator. The PCK is encrypted using the terminator's MCPTT ID and domain-specific material provided from the terminating user's KMS. The domain-specific key material of the terminator's KMS is identified by a KMS URI stored in the terminating user profile. The domain-specific key material for all KMSs is downloaded in advance from the initiator's home KMS as described in 3GPP TS 33.180 [78]. The PCK and PCK-ID are distributed within a MIKEY payload within the SDP offer of the private call request. This payload is called a MIKEY-SAKKE I_MESSAGE, as defined in IETF RFC 6509 [75], which ensures the confidentiality, integrity and authenticity of the payload. The encoding of the MIKEY payload in the SDP offer is described in IETF RFC 4567 [47] using an "a=key-mgmt" attribute. The payload is signed using a key associated to the identity of the initiating user. At the terminating side, the signature is validated. If valid, the UE extracts and decrypts the encapsulated PCK. The MCPTT UE also extracts the PCK-ID. This process is described in 3GPP TS 33.180 [78]. With the PCK successfully shared between the two MCPTT UEs, the UEs are able to use SRTP/SRTCP to create an end-to-end secure session.

For first-to-answer calls, the security context is initiated at call setup. An end-to-end security context is established that is unique to the pair of users involved in the call. The procedure involves transferral of an encapsulated private call key (PCK) and private call key id (PCK-ID) from the terminator to the initiator. The PCK is encrypted using the originator's MCPTT ID and domain-specific material provided from the originating user's KMS. The domain-specific key material of the originator's KMS is identified by a KMS URI stored in the originator's user profile. The domain-specific key material for all KMSs is downloaded in advance from the terminator's home KMS as described in 3GPP TS 33.180 [78]. The PCK and PCK-ID are distributed within a MIKEY payload within the SDP answer of the first-to-answer call response. This payload is called a MIKEY-SAKKE I_MESSAGE, as defined in IETF RFC 6509 [75], which ensures the confidentiality, integrity and authenticity of the payload. The encoding of the MIKEY payload included in the SDP answer using an "a=key-mgmt" attribute is described in IETF RFC 4567 [47]. The payload is signed using a key associated to the identity of the terminating user. At the originating side, the signature is validated. If valid, the UE extracts and decrypts the encapsulated PCK. The MCPTT UE also extracts the PCK-ID. This process is described in 3GPP TS 33.180 [78]. With the PCK successfully shared between the two MCPTT UEs, the UEs are able to use SRTP/SRTCP to create an end-to-end secure session.

End-to-end security is independent of the transmission path and hence is applicable to both on and off-network communications. With a security context established, the group call key and private call key can be used to encrypt media between the end-points as described in 3GPP TS 24.380 [5] clause 13.

4.7.2 Signalling security

Signalling security is established between the participating MCPTT function and the MCPTT client. This allows the following signalling to be integrity and confidentiality protected through the communication path between them:

- Signalling plane control (unicast only): Sensitive application data (as described in subclause 4.8)
- User plane control over unicast: Floor control messages
- User plane control over multicast: Floor control messages and MBMS subchannel control messages

NOTE 1: According to 3GPP TS 24.380 [5], currently the multicast floor control messages are Floor Idle and Floor Taken and the multicast MBMS subchannel control messages are Map Group To Bearer and Unmap Group To Bearer.

For unicast signalling between the participating MCPTT function and the MCPTT client, the signalling can be protected using the Client-Server Key (CSK), identified by a Client-Server Key Identifer (CSK-ID). The CSK and CSK-ID are initially uploaded from the MCPTT client to the MCPTT server within a MIKEY MIME payload within a SIP REGISTER message for service authorisation or a SIP PUBLISH message for service authorisation, as specified in subclause 9.2.1.3 of 3GPP TS 33.180 [78]. The CSK is confidentiality and integrity protected to the public service identity identifying the participating MCPTT function serving the MCPTT user and signed by the MCPTT ID of the MCPTT user.

The CSK and CSK-ID can also be updated by the participating MCPTT function. The procedure involves the participating MCPTT function generating a new CSK and CSK-ID and distributing the new key to the MCPTT client using a CSK 'key download' SIP MESSAGE, as specified in subclause 9.2.1.4 of 3GPP TS 33.180 [78]. The message contains a MIKEY MIME payload containing the CSK and CSK-ID. The CSK is confidentiality and integrity protected to the public service identity identifying the participating MCPTT function serving the MCPTT user and signed by the MCPTT ID of the MCPTT user. The client only uses a single CSK at any one time and discards the previously established CSK on receiving a new CSK.

In case of multicast, the protection of MBMS subchannel control messages on the general purpose MBMS subchannels can be done with MSCCKs (each identified by a corresponding MSCCK-ID), distributed during MBMS bearer announcement. Each general purpose MBMS subchannel is associated with an MSCCK and a corresponding MSCCK-ID. There can be multiple general purpose MBMS subchannels deployed, each associated with its own MSCCK and corresponding MSCCK-ID. The (MSCCK-ID, MSCCK) pair is provided for each general purpose MBMS subchannel separately.

The protection of floor control messages sent over MBMS subchannels can be done with Multicast Signalling Keys (MuSiK), (each identified by a corresponding (MuSiK-ID)), distributed via MuSiK download messages. The MSCCK and MuSiKs can be distributed independently of each other and in any order and can also be used independently. Signalling supports initial keying, as well as repeated re-keying and un-keying for both MSCCK and MuSiKs.

NOTE 2: When an MCPTT client interworks with a participating MCPTT function compliant only to Release 13 of the present document, the floor control messages can be protected using the MKFC and MKFC-ID as specified in 3GPP TS 24.380 [5].

The MuSiK download message contains an embedded MIME payload which is the MIKEY payload containing the MuSiK and MuSiK-ID, as well as an embedded XML payload potentially containing an explicit list of MCPTT group ids to which the key applies. Both payloads are protected as described in 3GPP TS 33.180 [78], as they are transferred between the participating MCPTT function and the MCPTT client. Within the XML payload, the list of MCPTT group ids is protected as application sensitive data (see subclause 4.8). Within the MIKEY payload, the MuSiK is encrypted using the MCPTT ID of the served MCPTT client. The payload is signed using a key associated to the identity of the participating MCPTT function. To distribute MuSiK, the participating MCPTT function uses the I_MESSAGE format from subclause 5.2.4 of 3GPP TS 33.180 [78], which includes associated parameters. The participating function sets the Status associated parameter to values defined in subclause E.6.9 of 3GPP TS 33.180 [78], namely "Not-revoked" when keying or rekeying and "Revoked" when unkeying, respectively. Upon receipt, the MCPTT client validates the signature and, if valid, the MCPTT client first examines the Status attribute and either marks the associated security functions as "not in use" or stores the MuSiK and the MuSiK-ID, and then replies with a success code; otherwise, the MCPTT client can reply with a failure code. if a success code is not received from the MCPTT client in response to the MuSiK download message , the participating MCPTT function starts using only unicast floor control signalling to the respective MCPTT client for the listed groups.

For MBMS subchannel control messages sent over the general purpose MBMS subchannel of an MBMS bearer, the MSCCK can be used. The the security context is initiated when the MBMS bearer is announced to the MCPTT clients. The procedure involves the participating MCPTT function creating an MBMS subchannel control key (MSCCK) and a correspondingkey identifier (MSCCK-ID) associated with the MBMS bearer when the MBMS bearer is activated, and then transferring the MSCCK and the MSCCK-ID associated with the MBMS bearer to served MCPTT clients using SIP signalling. The MSCCK is encrypted using the MCPTT ID of the served MCPTT client and domain-specific material provided from the KMS. The MSCCK and the MSCCK-ID associated with the MBMS bearer are distributed within a MIKEY payload within the SDP describing the general purpose MBMS subchannel of the MBMS bearer. This payload is called a MIKEY-SAKKE I_MESSAGE, as defined in IETF RFC 6509 [75], which ensures the confidentiality, integrity and authenticity of the payload. The encoding of the MIKEY payload in the SDP is described in IETF RFC 4567 [47] using an "a=key-mgmt" attribute. The payload is signed using a key associated to the identity of

the participating MCPTT function. To distribute MSCCK, the participating MCPTT function uses the I_MESSAGE format from subclause 5.2.4 of 3GPP TS 33.180 [78], which includes associated parameters. The participating function sets the Status associated parameter to values defined in subclause E.6.9 of 3GPP TS 33.180 [78], namely "Not-revoked" when keying or rekeying and "Revoked" when unkeying, respectively. Upon receipt, the MCPTT client validates the signature and, if the signature is found valid and the I_MESSAGE contains a Status attribute, the MCPTT client first examines the Status attribute and either marks the associated security functions as "not in use" or extracts and stores the encapsulated MSCCK and the corresponding MSCCK-ID. The decrypted key is used as described in 3GPP TS 33.180 [78]. With the MSCCK successfully shared between the participating MCPTT function and the served UEs, the participating MCPTT function is able to securely send MBMS subchannel control messages to the MCPTT clients.

4.8 Protection of sensitive application data.

In certain deployments, for example, in the case that the MCPTT operator uses the underlying SIP core infrastructure from the carrier operator, the MCPTT operator can prevent certain sensitive application data from being visible in the clear to the SIP layer. The following data are classed as sensitive application data:

- MCPTT ID;
- MCPTT group ID;
- user location information;
- emergency, alert and imminent-peril indicators;
- access token (containing the MCPTT ID); and
- MCPTT client ID.

The above data is transported as XML content in SIP messages. in XML elements or XML attributes.

Data is transported in attributes in the following circumstances in the procedures in the present document:

- an MCPTT ID, an MCPTT Group ID, and an MCPTT client ID in an XML document published in SIP PUBLISH request for affiliation according to IETF RFC 3856 [51];
- an MCPTT ID or an MCPTT Group ID in XML document notified in a SIP NOTIFY request for affiliation according to IETF RFC 3856 [51];
- an MCPTT ID in application/resource-lists+xml document included in an SIP INVITE request setting up a private call according to IETF RFC 5366 [20];
- an MCPTT ID in application/resource-lists+xml document included in an SIP INVITE request setting up a group call to a temporary group involving a non-controlling function that works in "Trusted Mode" according to IETF RFC 5366 [20], whereby the participants are returned to the controlling function in a MIME body of a SIP 403 (Forbidden) with the P-Refused-URI-List header field according to IETF RFC 5318 [36];
- an MCPTT ID in XML document provided in SIP NOTIFY request of a conference event package according to IETF RFC 4575 [30]; and
- an MCPTT ID or MCPTT Group ID in application/resource-lists+xml document according to IETF RFC 5366 [20], included in a SIP REFER request when using a pre-established session (the application/resource-lists+xml MIME body is pointed to by a Cid-URL as specified in IETF RFC 2392 [62] contained in the Refer-To header field of the SIP REFER request);

3GPP TS 33.180 [78] describes a method to provide confidentiality protection of sensitive application data in elements by using XML encryption (i.e. xmlenc) and in attributes by using an attribute confidentiality protection scheme described in subclause 6.6.2.3 of the present document. Integrity protection can also be provided by using XML signatures (i.e. xmlsig).

Protection of the data relies on a shared XML protection key (XPK) used to encrypt and sign data:

- between the MCPTT client and the MCPTT server, the XPK is a client-server key (CSK); and
- between MCPTT servers and between MCPTT domains, the XPK is a signalling protection key (SPK).

The CSK (XPK) and a key-id CSK-ID (XPK-ID) are generated from keying material provided by the key management server. Identity based public key encryption based on MIKEY-SAKKE is used to transport the CSK between SIP end-points. The encrypted CSK is transported from the MCPTT client to the MCPTT server when the MCPTT client performs service authorisation as described in clause 7 and is also used during service authorisation to protect the access token.

The SPK (XPK) and a key-id SPK-ID (XPK-ID) are directly provisioned in the MCPTT servers.

Configuration in the MCPTT client and MCPTT server is used to determine whether one or both of confidentiality protection and integrity protection are required.

The following four examples give a brief overview of the how confidentiality and integrity protection is applied to application data in this specification.

EXAMPLE 1: Pseudo code showing how confidentiality protection is represented in the procedures in the document for sensitive data sent by the originating client.

```
IF configuration is set for confidentiality protection of sensitive data
THEN
    Encrypt data element using the CSK (XPK) by following TS 33.180;
    Include in an <EncryptedData> element of the XML MIME body according to TS 33.180:
      (1) the encryption method;
      (2) the key-id (XPK-ID);
      (3) the cipher data;
    Encrypt URIs in attribute using the CSK (XPK) by following subclause 6.6.2.3;
ELSE
    include application data into XML MIME body in clear text;
ENDIF;
```

EXAMPLE 2: Pseudo code showing how integrity protection is represented in the procedures in the present document for data sent by the originating client.

```
IF configuration is set for integrity protection of application data
THEN
    Use a method to hash the content as specified in TS 33.180;
    Generate a signature for the hashed content using the CSK (XPK) as specified in TS 33.180;
    Include within a <Signature> XML element of the XML MIME body according to TS 33.180:
       (1) a cannonicalisation method to be applied to the signed information;
       (2) the signature method used for generating the signature;
       (3) a reference to the content to be signed;
       (4) the hashing method used;
       (5) the hashed content;
       (6) the key-id (XPK-ID);
       (7) the signature value;
ENDIF;
```

EXAMPLE 3: Pseudo code showing how confidentiality protection is represented in the procedures in the present document at the server side when receiving encrypted content.

```
IF configuration is set for confidentiality protection of sensitive data
THEN
    Check that the XML content contains the <EncryptedData> element;
    Check that the XML document contains a URI with the domain name for MCPTT confidentiality
protection;
    Return an error if the <EncryptedData> element or domain name for MCPTT confidentiality
protection are not found;
    Otherwise:
       (1) obtain the CSK (XPK) using the CSK-ID (XPK-ID) in the received XML body;
       (2) for encrypted data in elements, decrypt the data elements using the CSK as specified
in TS 33.180 as required;
       (3) for encrypted URIs in attributes, decrypt the URIs using the CSK as specified in
subclause 6.6.2.3;
ENDIF;
```

EXAMPLE 4: Pseudo code showing how integrity protection is represented in the procedures in the present document at the server side when receiving signed content.

```
IF configuration is set for integrity protection of application data
THEN
   Check that the XML content contains the <Signature> element;
```

```
      Return an error if the <Signature> element is not found;
      Otherwise:
          (1) obtain the CSK (XPK) using the CSK-ID (XPK-ID) in the received XML body;
          (2) verify the signature of the content using the CSK;
      Return an error if the validation of the signature fails;
      IF validation of the signature passes
      THEN
         decrypt any data found in <EncryptedData> elements;
         decrypt any encrypted URIs found in attributes;
      ENDIF;
   ENDIF;
```

The content can be re-encrypted and signed again using the SPK between MCPTT servers.

The following examples show the difference between normal and encrypted data content. In this example consider the MCPTT client initiating a prearranged group session.

EXAMPLE 5: <mcptt-info> MIME body represented with data elements in the clear:

```
Content-Type: application/vnd.3gpp.mcptt-info+xml
<?xml version="1.0"?>
<mcptt-info>
  <mcptt-Params>
    <session-type>prearranged</session-type>
    <mcptt-request-uri type="Normal">
      <mcpttURI>sip:group123@mcpttoperator1.com></mcpttURI>
    </mcptt-request-uri>
  </mcptt-Params>
</mcptt-info>
```

EXAMPLE 6: <mcptt-info> MIME body represented with the <mcptt-request-uri> encrypted:

```
Content-Type: application/vnd.3gpp.mcptt-info+xml
<?xml version="1.0"?>
<mcptt-info>
  <mcptt-Params>
    <session-type>prearranged</session-type>
    <mcptt-request-uri type="Encrypted">
      <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
       Type='http://www.w3.org/2001/04/xmlenc#Content'>
        <EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
        <ds:KeyInfo>
          <ds:KeyName>base64XpkId</KeyName>
        </ds:KeyInfo>
        <CipherData>
          <CipherValue>A23B45C5657689090</CipherValue>
        </CipherData>
      </EncryptedData>
    </mcptt-request-uri>
  </mcptt-Params>
</mcptt-info>
```

EXAMPLE 7: pidf+xml MIME body represented with clear URIs in attributes:

```
Content-Type: application/pidf+xml
<?xml version="1.0" encoding="UTF-8"?>
<presence entity="sip:somebody@mcptt.org">
  <tuple id="acD4rhU87bK">
    <status>
      <affiliation group="sip:thegroup@mcptt.org"/>
    </status>
  </tuple>
</presence>
```

EXAMPLE 8: pidf+xml MIME body represented with encrypted URIs in attributes:

```
Content-Type: application/pidf+xml
<?xml version="1.0" encoding="UTF-8"?>
<presence entity="sip:c4Hrt45XG8IohRFT67vfdr3V;iv=45RtfVgHY23k8Ihy;xpk-id=b7UJv9;alg=128-aes-
gcm@mc1-encryption.3gppnetwork.org">
  <tuple id="acD4rhU87bK">
    <status>
      <affiliation group="sip:98yudFG45tx_89TYGedb4ujF ;iv=FGD567kjhfH7d4-D;key-id=eV9kl7;alg=128-
aes-gcm@mc1-encryption.3gppnetwork.org"/>
    </status>
  </tuple>
```

```
</presence>
```

4.9 Pre-established session

When establishing a pre-established session, the MCPTT client negotiates the media parameters, including establishing IP addresses and ports using interactive connectivity establishment (ICE) as specified in IETF RFC 5245 [17] with the participating MCPTT function, prior to using the pre-established session for establishing MCPTT sessions with other MCPTT users. The procedures for establishing, modifying and releasing a pre-established session are defined in clause 8.

The pre-established session can later be used in MCPTT calls. This avoids the need to negotiate media parameters (including evaluating ICE candidates) and reserving bearer resources during the MCPTT call establishment that results in delayed MCPTT call establishment.

The use of pre-established session on the origination side is compatible with the use of on demand session on the termination side. The use of pre-established session on the termination side is compatible with the use of on demand session on the origination side.

The MCPTT client procedures for:

- leaving a MCPTT session using a pre-established session that was initiated by the MCPTT client are defined in subclause 6.2.4.2;
- releasing a MCPTT session using a pre-established session that was initiated by the MCPTT client are defined in subclause 6.2.5.2;
- establishing a pre-arranged group call using a pre-established session are defined in subclause 10.1.1.2.2;
- rejoining a pre-arranged group call using a pre-established session are defined in subclause 10.1.1.2.4.2;
- joining a chat MCPTT group session using a pre-established session are defined in subclause 10.1.2.2.2;
- establishing a private call using a pre-established session are defined in subclause 11.1.1.2.2; and
- releasing a private call using a pre-established session are defined in subclause 11.1.3.1.2.

The participating MCPTT function procedures for:

- establishing a MCPTT session using automatic commencement mode are defined in subclause 6.3.2.2.5.3;
- establishing a MCPTT session using manual commencement mode are defined in subclause 6.3.2.2.6.3;
- releasing a MCPTT session using a pre-established session are defined in subclause 6.3.2.2.8.2;
- establishing a pre-arranged group call using a pre-established session are defined in subclause 10.1.1.3.1.2;
- releasing a pre-arranged group call using a pre-established session are defined in subclause 10.1.1.3.3.2;
- rejoining a pre-arranged group call using a pre-established session are defined in subclause 10.1.1.3.5.2;
- establishing a MCPTT group session using a pre-established session are defined in subclause 10.1.2.3.2;
- originating a private call from a MCPTT client using a pre-established session are defined in subclause 11.1.1.3.1.2;
- establishing a private call to a MCPTT client using a pre-established session are defined in subclause 11.1.1.3.2;
- releasing a private call initiated by the served MCPTT client using a pre-established session are defined in subclause 11.1.3.2.1.2; and
- releasing a private call initiated by the remote MCPTT client using a pre-established session are defined in subclause 11.1.3.2.2.2.

4.10 MCPTT client ID

The MCPTT client assigns the MCPTT client ID when the MCPTT client is used for the first time. The MCPTT client generates the MCPTT client ID as specified in subclause 4.2 of IETF RFC 4122 [67].

The MCPTT client preserves the MCPTT client ID:

- while the MCPTT client is SIP registered as specified in 3GPP TS 24.229 [4];
- while the MCPTT client is not SIP registered as specified in 3GPP TS 24.229 [4] and the UE serving the MCPTT client is switched on;
- while the UE serving the MCPTT client is switched off; and
- while the UE serving the MCPTT client is power-cycled.

NOTE: MCPTT client ID is not preserved when the UE is reset to factory settings.

4.11 Off-network MCPTT

Off-network services are available for the user if the value of "/<*x*>/<*x*>/OffNetwork/Authorised" leaf node present in user profile as specified in 3GPP TS 24.483 [45] is set to "true".

4.12 Broadcast Group Calls

A broadcast group call is a group call where the initiating MCPTT user expects no response from the other MCPTT users, so that when the user's transmission is complete, so is the call. The functionality in the present release of the specification for broadcast group calls is not compliant to the requirements for user-broadcast group and group-broadcast group calls as specified in 3GPP TS 22.179 [2], 3GPP TS 22.280 [76] and 3GPP TS 23.379 [3]. In the present release of the specification, a broadcast group call can be initiated by an MCPTT user on any MCPTT group that the MCPTT user is part of.

NOTE 1: Configuration related to the authorisation to create a user-broadcast group or a group-broadcast exists in the user profile document as specified in 3GPP TS 24.484 [50], but is not used by any procedures in 3GPP TS 24.481 [31] in the current release, as the ability for an authorised user to create user-broadcast groups and group-broadcast groups is not provided in the current release.

NOTE 2: Configuration related to broadcast group hierarchies can be found in the group document as specified in 3GPP TS 24.481 [31] and in the service configuration document as specified in 3GPP TS 24.484 [50]. However, this configuration is not used by any procedures in 3GPP TS 24.380 [5] in the current release.

5 Functional entities

5.1 Introduction

This clause associates the functional entities with the MCPTT roles described in the stage 2 architecture document (see 3GPP TS 23.379 [3]).

5.2 MCPTT client

To be compliant with the procedures in the present document, an MCPTT client shall:

- act as the user agent for all MCPTT application transactions (e.g. initiation of a group call); and
- support handling of the MCPTT client ID as described in subclause 4.10.

To be compliant with the on-network procedures in the present document, an MCPTT client shall:

- support the MCPTT client on-network procedures defined in 3GPP TS 23.379 [3];
- support the GCS UE procedures defined in 3GPP TS 23.468 [57] for unicast delivery, MBMS delivery and service continuity;
- act as a SIP UA as defined in 3GPP TS 24.229 [4];
- generate SDP offer and SDP answer in accordance with 3GPP TS 24.229 [4] and subclause 6.2;
- act as a floor participant responsible for floor requests and implement the on-network procedures for floor requests as specified in 3GPP TS 24.380 [5];
- for registration and service authorisation, implement the procedures specified in subclause 7.2;
- for pre-established sessions, implement the procedures specified in subclause 8.2.1, subclause 8.3.1, subclause 8.4.1, and the procedures specified in 3GPP TS 24.380 [5];
- for affiliation, implement the procedures specified in subclause 9.2;
- for group call functionality (including broadcast, emergency and imminent peril), implement the MCPTT client procedures specified in subclause 10.1; and
- for private call functionality (including emergency), implement the MCPTT client procedures specified in subclause 11.1;
- for emergency alert, implement the procedures specified in subclause 12.1;
- for location reporting, implement the procedures specified in subclause 13.3; and
- for MBMS transmission usage, implement the procedures in subclause 14.3.

To be compliant with the off-network procedures in the present document, an MCPTT client shall:

- support the off-network procedures defined in 3GPP TS 23.379 [3];
- support the MCPTT off-network protocol (MONP) defined in clause 15;
- act as a floor participant for floor requests and implement the off-network procedures for floor requests as specified in 3GPP TS 24.380 [5];
- act as a floor control server providing distributed floor control and implement the off-network procedures for floor control as specified in 3GPP TS 24.380 [5];
- implement the procedures for ProSe direct discovery for public safety use as specified in 3GPP TS 24.334 [28];
- implement the procedures for one-to-one ProSe direct communication for Public Safety use as specified in 3GPP TS 24.334 [28];
- for group call functionality (including emergency and imminent peril), implement the MCPTT client procedures specified in subclause 10.2;
- for broadcast group call functionality implement the procedures specified in subclause 10.3; and
- for private call functionality (including emergency), implement the MCPTT client procedures specified in subclause 11.2.

To be compliant with the service continuity procedures in the present document, an MCPTT client shall:

- implement the registration requirements for service continuity as specified in subclause 7.2.1; and
- implement the procedures specified in clause 14A.

To be compliant with the on-network and off-network procedures in the present document requiring end-to-end private call security key distribution, an MCPTT client shall support the procedures specified in 3GPP TS 33.179 [46].

To be compliant with the procedures for confidentiality protection of XML elements in the present document, the MCPTT client shall implement the procedures specified in subclause 6.6.2.

To be compliant with the procedures for integrity protection of XML MIME bodies in the present document, the MCPTT client shall implement the procedures specified in subclause 6.6.3.

5.3 MCPTT server

5.3.1 General

An MCPTT server can perform the controlling role for group calls and private calls as defined in 3GPP TS 23.379 [3].

An MCPTT server can perform the participating role for group calls and private calls as defined in 3GPP TS 23.379 [3].

An MCPTT server can perform a non-controlling role for temporary group calls involving groups from multiple MCPTT systems as specified in 3GPP TS 23.379 [3].

An MCPTT server can perform a non-controlling role for temporary group calls involving groups only from the primary MCPTT system.

An MCPTT server performing the participating role can serve an originating MCPTT user.

An MCPTT server performing the participating role can serve a terminating MCPTT user.

The same MCPTT server can perform the participating role and controlling role for the same group session.

The same MCPTT server can perform the participating role and non-controlling role for the same group session.

When referring to the procedures in the present document for the MCPTT server acting in a participating role for the served user, the term, "participating MCPTT function" is used.

When referring to the procedures in the present document for the MCPTT server acting in a controlling role for the served user, the term "controlling MCPTT function" is used.

When referring to the procedures in the present document for the MCPTT server acting in a non-controlling role for a group call, the term "non-controlling MCPTT function of an MCPTT group" is used.

To be compliant with the procedures in the present document, an MCPTT server shall:

- support the MCPTT server procedures defined in 3GPP TS 23.379 [3];
- implement the role of an AS performing 3rd party call control acting as a routing B2BUA as defined in 3GPP TS 24.229 [4];
- support the GCS AS procedures defined in 3GPP TS 23.468 [57] for unicast delivery, MBMS delivery and service continuity;
- generate SDP offer and SDP answer in accordance with 3GPP TS 24.229 [4] and subclause 6.3;
- implement the role of a centralised floor control server and implement the on-network procedures for floor control as specified in 3GPP TS 24.380 [5];
- for registration and service authorisation, implement the procedures specified in subclause 7.3;
- for pre-established sessions, implement the procedures specified in subclause 8.2.2, subclause 8.3.2, subclause 8.4.2 and the procedures specified in 3GPP TS 24.380 [5];
- for affiliation, implement the procedures specified in subclause 9.2.2;
- for group call functionality (including broadcast, emergency and imminent peril), implement the MCPTT server procedures specified in subclause 10.1;
- for private call functionality (including emergency), implement the MCPTT server procedures specified in subclause 11.1; and
- for priority sharing, implement the MCPTT server procedures in subclause 6.7.

To be compliant with the procedures in the present document requiring the distribution of private call keying material between MCPTT clients as specified in 3GPP TS 33.180 [78], an MCPTT server shall ensure that the keying material is copied from incoming SIP messages into the outgoing SIP messages.

To be compliant with the procedures for confidentiality protection of XML elements in the present document, the MCPTT server shall implement the procedures specified in subclause 6.6.2.

To be compliant with the procedures for integrity protection of XML MIME bodies in the present document, the MCPTT server shall implement the procedures specified in subclause 6.6.3.

5.3.2 Functional connectivity models

The following figures give an overview of the connectivity between the different functions of the MCPTT server as described in subclause 5.3.1.

NOTE: Separate boxes are shown for each of the functions of the MCPTT server. In each MCPTT system, these functions can be physically combined into one MCPTT server or can be implemented on more than one MCPTT server. For example, there could be an instantiation of an MCPTT server that only serves as a controlling MCPTT function, but not as a participating MCPTT function for any MCPTT clients. When an MCPTT server supports more than one function, then sending requests from one function to another does not incur a traversal of the underlying IMS SIP core network.

Figure 5.3.2-1 shows the basic functions of the MCPTT server when operating within the primary MCPTT system.

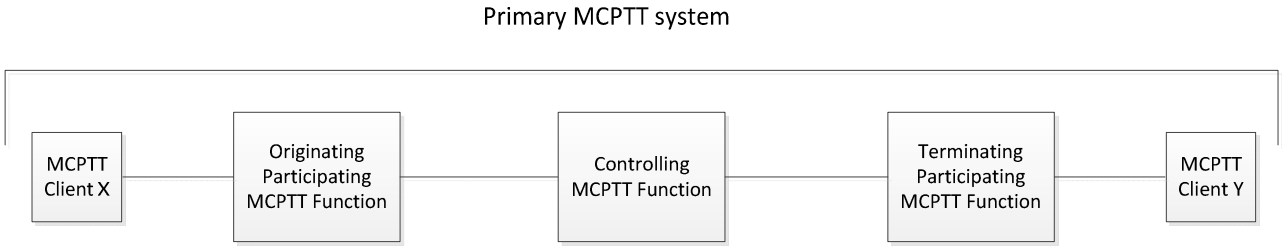

Figure 5.3.2-1: Functions of the MCPTT server in the primary MCPTT system

Figure 5.3.2-2 shows the use of the non-controlling MCPTT function of an MCPTT group within the primary MCPTT system. This can occur due to group re-grouping of groups within the same MCPTT system, where the MCPTT server(s) of one or more of the constituent groups are not controlled by the same controlling MCPTT function as that of the temporary group. The non-controlling MCPTT function of an MCPTT group either provide the identities of the users of the group to the controlling MCPTT function, or the non-controlling MCPTT function of an MCPTT group can invite the users of the group on behalf of the controlling MCPTT function.

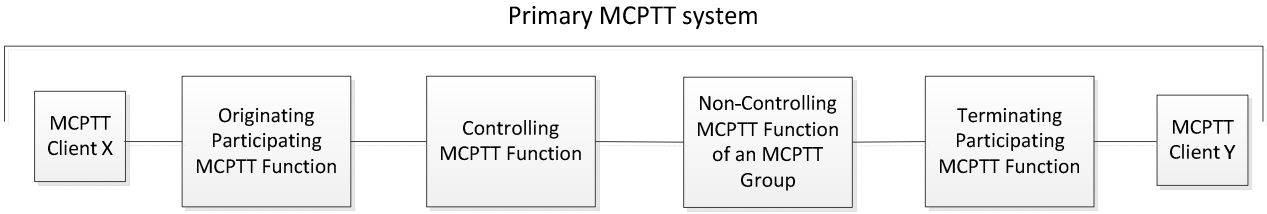

Figure 5.3.2-2: The non-controlling function operating in the primary MCPTT system

Figure 5.3.2-3 shows the roles of the MCPTT server in a mutual aid relationship between a primary MCPTT system and a partner MCPTT system. Here, the controlling MCPTT function is in the primary MCPTT system and the called user is homed in a partner MCPTT system.

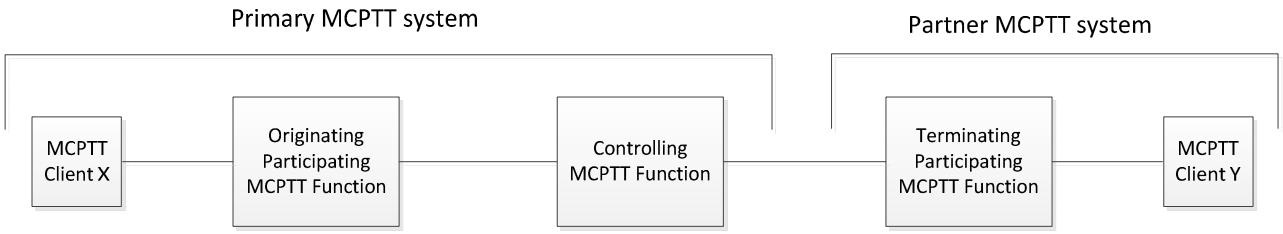

Figure 5.3.2-3: Mutual aid relationship between the primary MCPTT system and a partner MCPTT system with the controlling MCPTT function in the primary MCPTT system

Figure 5.3.2-4 shows the roles of the MCPTT server in a mutual aid relationship between a primary MCPTT system and a partner MCPTT system. Here, the controlling MCPTT function is in the partner MCPTT system.

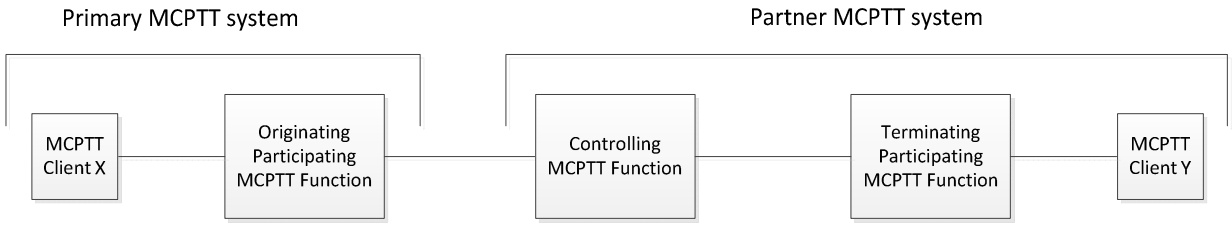

Figure 5.3.2-4: Mutual aid relationship between the primary MCPTT system and a partner MCPTT system with the controlling MCPTT function in the partner MCPTT system

Figure 5.3.2-5 shows the roles of the MCPTT server in a mutual aid relationship between a primary MCPTT system and a partner MCPTT with the use of a non-controlling MCPTT function of an MCPTT group within the partner MCPTT system. This can occur due to group re-grouping where the MCPTT server(s) of one or more of the constituent groups are homed on the partner system. If the primary MCPTT system and partner MCPTT system operate in a trusted mutual aid relationship, then the non-controlling MCPTT function of an MCPTT group can provide the identities of the users of the group to the controlling MCPTT function. If the primary MCPTT system and partner MCPTT system operate in an untrusted mutual aid relationship, then the non-controlling MCPTT function of an MCPTT group invites the users of the group on behalf of the controlling MCPTT function.

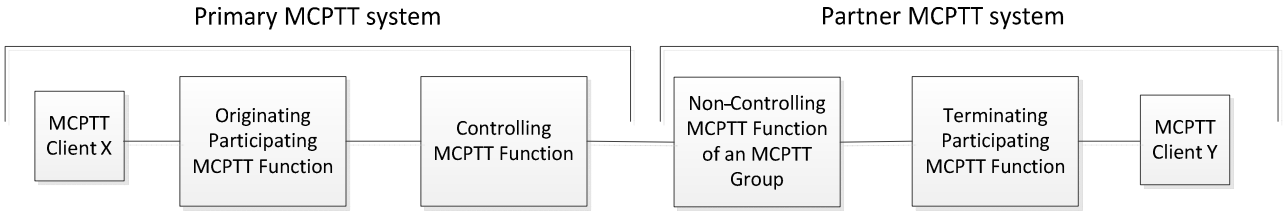

Figure 5.3.2-5: Mutual aid relationship between the primary MCPTT system and a partner MCPTT system involving the use of a non-controlling MCPTT function of an MCPTT group in the partner MCPTT system

Figure 5.3.2-6 illustrates a functional connectivity model involving multiple partner systems where the partner system that owns the group does not home any of the group members.

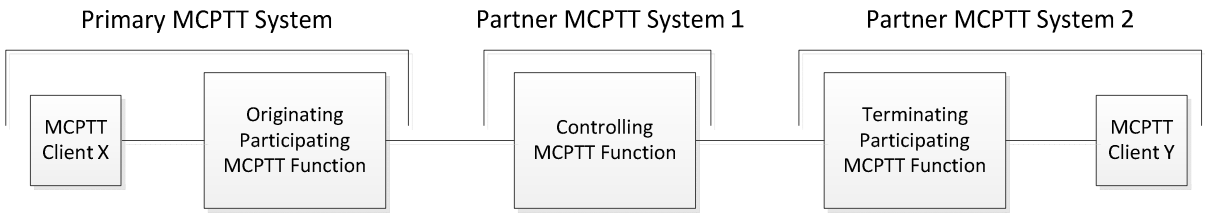

Figure 5.3.2-6: : Mutual aid relationship between the primary MCPTT system and more than one partner MCPTT system

Other functional connectivity models can exist.

5.3.3 Failure case

When initiating a failure response to any received request, depending on operator policy, the MCPTT server may insert a SIP Response-Source header field with an "fe" header field parameter constructed with the URN namespace "urn:3gpp:fe", the fe-id part of the URN set to "as" and the "role" header field parameter set to "pf-mcptt-server", "cf-mcptt-server" or "ncf-mcptt-server" depending on the current role endorsed by the MCPTT server and in accordance with subclause 7.2.17 of 3GPP TS 24.229 [4].

5.3.4 Management of MBMS bearers

When providing services over MBMS, an MCPTT server acting in the participating MCPTT function role shall:

- allocate TMGIs and activate MBMS bearers in MBMS service areas to be used for MCPTT media and media control distribution via multicast, per 3GPP TS 23.468 [57] and 3GPP TS 29.468 [42];
- deactivate MBMS bearers and deallocate TMGIs when no longer necessary, per 3GPP TS 23.468 [57] and 3GPP TS 29.468 [42];
- handle MBMS bearers related notifications per 3GPP TS 23.468 [57] and 3GPP TS 29.468 [42]; and
- adjust the priority / pre-emption characteristics of MBMS bearers, as appropriate, in reponse to relevant events (e.g. emergency or imminent peril call), using procedures specified in per 3GPP TS 23.468 [57] and 3GPP TS 29.468 [42].

5.4 MCPTT UE-to-network relay

To be compliant with the procedures in the present document for service continuity, an MCPTT UE- to-network relay shall support the UE-to-network relay procedures as specified in 3GPP TS 24.334 [28] and 3GPP TS 23.379 [3].

6 Common procedures

6.1 Introduction

This clause describes the common procedures for each functional entity as specified.

6.2 MCPTT client procedures

6.2.0 Distinction of requests at the MCPTT client

6.2.0.1 SIP MESSAGE request

The MCPTT client needs to distinguish between the following SIP MESSAGE requests:

- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt-location-info+xml" and includes an XML body containing a Location root element containing a Configuration element. Such requests are known as "SIP MESSAGE request for location report configuration" in the present document;
- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt-location-info+xml" and includes an XML body containing a Location root element containing a Request element. Such requests are known as "SIP MESSAGE request for location report request" in the present document.

- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt -info+xml" and includes an XML body containing a <mcptt-info> root element containing the <mcptt-Params> element and an <anyExt> element containing the <request-type> element set to a value of "private-call-call-back-request". Such requests are known as "SIP MESSAGE request for private call call-back request for terminating client";

- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt -info+xml" and includes an XML body containing a <mcptt-info> root element containing the <mcptt-Params> element and an <anyExt> element containing the <request-type> element set to a value of "private-call-call-back-cancel-request". Such requests are known as "SIP MESSAGE request for private call call-back cancel request for terminating client";

- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt -info+xml" and includes an XML body containing a <mcptt-info> root element containing the <mcptt-Params> element and an <anyExt> element containing the <response-type> element set to a value of "private-call-call-back-response". Such requests are known as "SIP MESSAGE request for private call call-back response for terminating client";

- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt -info+xml" and includes an XML body containing a <mcptt-info> root element containing the <mcptt-Params> element and an <anyExt> element containing the <response-type> element set to a value of "private-call-call-back-cancel-response". Such requests are known as "SIP MESSAGE request for private call call-back cancel response for terminating client";

- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt -info+xml" and includes an XML body containing a <mcptt-info> root element containing the <mcptt-Params> element and an <anyExt> element containing the <request-type> element set to a value of "group-selection-change-request". Such requests are known as "SIP MESSAGE request for group selection change request for terminating client";

- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt -info+xml" and includes an XML body containing a <mcptt-info> root element containing the <mcptt-Params> element and an <anyExt> element containing the <response-type> element set to a value of "group-selection-change-response". Such requests are known as "SIP MESSAGE request for group selection change response for terminating client"; and

- SIP MESSAGE request routed to the MCPTT client as a result of initial filter criteria containing a Content-Type header field set to "application/mikey" and a CSB-ID containing a CSK-ID. Such requests are known as "SIP MESSAGE request for CSK download for terminating client".

6.2.1 SDP offer generation

The SDP offer shall contain only one SDP media-level section for MCPTT speech according to 3GPP TS 24.229 [4] and, if floor control shall be used during the session, shall contain one SDP media-level section for a media-floor control entity according to 3GPP TS 24.380 [5].

When composing an SDP offer according to 3GPP TS 24.229 [4] the MCPTT client:

1) shall set the IP address of the MCPTT client for the offered MCPTT speech media stream and, if floor control shall be used, for the offered media-floor control entity;

NOTE: If the MCPTT client is behind a NAT the IP address and port included in the SDP offer can be a different IP address and port than the actual IP address and port of the MCPTT client depending on the NAT traversal method used by the SIP/IP Core.

2) shall include an "m=audio" media-level section for the MCPTT media stream consisting of:

   a) the port number for the media stream selected; and

   b) the codec(s) and media parameters and attributes with the following clarification:

      i) if the MCPTT client is initiating a call to a group identity;

ii) if the <preferred-voice-encodings> element is present in the group document retrieved by the group management client as specified in 3GPP TS 24.481 [31] containing an <encoding> element with a "name" attribute; and

iii) if the MCPTT client supports the encoding name indicated in the value of the "name" attribute;

then the MCPTT client:

i) shall insert the value of the "name" attribute in the <encoding name> field of the "a=rtpmap" attribute as defined in IETF RFC 4566 [12];

c) if the SDP offer is for an ambient listening call:

i) if this is a remotely initiated ambient listening call, include an "a=recvonly" attribute; or

ii) if this is a locally initiated ambient listening call, include an "a=sendonly" attribute; and

d) "i=" field set to "speech" according to 3GPP TS 24.229 [4];

3) if floor control shall be used during the session, shall include an "m=application" media-level section as specified in 3GPP TS 24.380 [5] clause 12 for a media-floor control entity, consisting of:

a) the port number for the media-floor control entity selected as specified in 3GPP TS 24.380 [5]; and

b) the 'fmtp' attributes as specified in 3GPP TS 24.380 [5] clause 14; and

4) if end-to-end security is required for a private call and the SDP offer is not for establishing a pre-established session, shall include the MIKEY-SAKKE I_MESSAGE in an "a=key-mgmt" attribute as a "mikey" attribute value in the SDP offer as specified in IETF RFC 4567 [47].

6.2.2 SDP answer generation

When the MCPTT client receives an initial SDP offer for an MCPTT session, the MCPTT client shall process the SDP offer and shall compose an SDP answer according to 3GPP TS 24.229 [4].

When composing an SDP answer, the MCPTT client:

1) shall accept the MCPTT speech media stream in the SDP offer;

2) shall set the IP address of the MCPTT client for the accepted MCPTT speech media stream and, if included in the SDP offer, for the accepted media-floor control entity;

NOTE: If the MCPTT client is behind a NAT the IP address and port included in the SDP answer can be a different IP address and port than the actual IP address and port of the MCPTT client depending on the NAT traversal method used by the SIP/IP Core.

3) shall include an "m=audio" media-level section for the accepted MCPTT speech media stream consisting of:

a) the port number for the media stream;

b) media-level attributes as specified in 3GPP TS 24.229 [4];

c) if the "a=recvonly" attribute is present in the SDP offer, include an "a=sendonly" attribute;

d) if the "a=sendonly" attribute is present in the SDP offer, include an "a=recvonly" attribute; and

e) "i=" field set to "speech" according to 3GPP TS 24.229 [4];

4) if included in the SDP offer, shall include the media-level section of the offered media-floor control entity consisting of:

a) an "m=application" media-level section as specified in 3GPP TS 24.380 [5] clause 12; and

b) 'fmtp' attributes as specified in 3GPP TS 24.380 [5] clause 14; and

5) if end-to-end security is required for a first-to-answer call, shall include the MIKEY-SAKKE I_MESSAGE in an "a=key-mgmt" attribute as a "mikey" attribute value in the SDP answer as specified in 3GPP TS 33.180 [78].

6.2.3 Commencement modes

6.2.3.1 Automatic commencement mode

6.2.3.1.1 Automatic commencement mode for private calls

When performing the automatic commencement mode procedures, the MCPTT client:

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

2) shall include the option tag "timer" in a Require header field of the SIP 200 (OK) response;

3) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP 200 (OK) response;

4) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP 200 (OK) response;

5) shall include the Session-Expires header field in the SIP 200 (OK) response and start the SIP session timer according to IETF RFC 4028 [7]. The "refresher" parameter in the Session-Expires header field shall be set to "uas";

6) shall, if the incoming SIP INVITE request contains a Replaces header field, include in the SDP answer in the SIP 200 (OK) response to the SDP offer the parameters used for the pre-established session identified by the contents of the Replaces header field;

7) shall, if the incoming SIP INVITE request does not contain a Replaces header field, include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP INVITE request according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.2;

NOTE: In the case of a new emergency call where the terminating client is using a pre-established session, the SIP INVITE request containing a Replaces header is used to replace the pre-established session.

8) shall send the SIP 200 (OK) response towards the MCPTT server according to rules and procedures of 3GPP TS 24.229 [4];

9) shall, if the incoming SIP INVITE request contains a Replaces header field, release the pre-established session identified by the contents of the Replaces header field; and

10) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.2.

When NAT traversal is supported by the MCPTT client and when the MCPTT client is behind a NAT, generation of SIP responses is done as specified in this subclause and as specified in IETF RFC 5626 [15].

6.2.3.1.2 Automatic commencement mode for group calls

When performing the automatic commencement mode procedures, the MCPTT client shall follow the procedures in subclause 6.2.3.1.1 with the following clarification:

- The MCPTT client may include a P-Answer-State header field with the value "Confirmed" as specified in IETF RFC 4964 [34] in the SIP 200 (OK) response.

6.2.3.2 Manual commencement mode

6.2.3.2.1 Manual commencement mode for private calls

When performing the manual commencement mode procedures:

1) if the MCPTT user declines the MCPTT session invitation the MCPTT client shall send a SIP 480 (Temporarily Unavailable) response towards the MCPTT server with the warning text set to: "110 user declined the call invitation" in a Warning header field as specified in subclause 4.4, and not continue with the rest of the steps in this subclause.

The MCPTT client:

1) shall accept the SIP INVITE request and generate a SIP 180 (Ringing) response according to rules and procedures of 3GPP TS 24.229 [4];

2) shall include the option tag "timer" in a Require header field of the SIP 180 (Ringing) response;

3) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP 180 (Ringing) response;

4) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP 180 (Ringing) response; and

5) shall send the SIP 180 (Ringing) response to the MCPTT server.

When sending the SIP 200 (OK) response to the incoming SIP INVITE request, the MCPTT client shall follow the procedures in subclause 6.2.3.1.1.

When NAT traversal is supported by the MCPTT client and when the MCPTT client is behind a NAT, generation of SIP responses is done as specified in this subclause and as specified in IETF RFC 5626 [15].

6.2.3.2.2 Manual commencement mode for group calls

When performing the manual commencement mode procedures:

1) the terminating MCPTT client may automatically generate a SIP 183 (Session Progress) in accordance with 3GPP TS 24.229 [4], prior to the MCPTT user's acknowledgement; and

2) if the MCPTT user declines the MCPTT session invitation the MCPTT client shall send a SIP 480 (Temporarily Unavailable) response towards the MCPTT server with the warning text set to: "110 user declined the call invitation" in a Warning header field as specified in subclause 4.4, and not continue with the rest of the steps in this subclause.

When generating a SIP 183 (Session Progress) response, the MCPTT client:

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

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

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

2) may include a P-Answer-State header field with the value "Unconfirmed" as specified in IETF RFC 4964 [34];

When sending the SIP 200 (OK) response to the incoming SIP INVITE request, the MCPTT client shall follow the procedures in subclause 6.2.3.1.2.

When NAT traversal is supported by the MCPTT client and when the MCPTT client is behind a NAT, generation of SIP responses is done as specified in this subclause and as specified in IETF RFC 5626 [15].

6.2.4 Leaving an MCPTT session initiated by MCPTT client

6.2.4.1 On-demand session case

Upon receiving a request from an MCPTT user to leave an MCPTT session established using on-demand session signalling, the MCPTT client:

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

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

3) shall set the Request-URI to the MCPTT session identity to leave; and

4) shall send a SIP BYE request towards MCPTT server according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the SIP BYE request, the MCPTT client shall interact with the media plane as specified in 3GPP TS 24.380 [5].

6.2.4.2 Pre-established session case

Upon receiving a request from an MCPTT user to leave an MCPTT session within a pre-established session, the MCPTT client:

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

2) shall generate an initial SIP REFER request outside a dialog in accordance with the procedures specified in 3GPP TS 24.229 [4], IETF RFC 4488 [22] and IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27];

3) shall set the Request-URI of the SIP REFER request to the public service identity identifying the pre-established session on the MCPTT server serving the MCPTT user;

4) shall include the Refer-Sub header field with value "false" according to rules and procedures of IETF RFC 4488 [22];

5) shall include the Supported header field with value "norefersub" according to rules and procedures of IETF RFC 4488 [22];

6) shall set the Refer-To header field of the SIP REFER request to the MCPTT session identity to leave;

7) shall include the "method" SIP URI parameter with the value "BYE" in the URI in the Refer-To header field;

8) shall include a Target-Dialog header field as specified in IETF RFC 4538 [23] identifying the pre-established session; and

9) shall send the SIP REFER request according to 3GPP TS 24.229 [4].

Upon receiving a SIP 2xx response to the SIP REFER request, the MCPTT client shall interact with media plane as specified in 3GPP TS 24.380 [5].

6.2.5 Releasing an MCPTT session initiated by MCPTT client

6.2.5.1 On-demand session case

When the MCPTT client wants to release an MCPTT session established using on-demand session signalling, the MCPTT client:

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

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

3) shall set the Request-URI to the MCPTT session identity to release; and

4) shall send a SIP BYE request towards MCPTT server according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the SIP BYE request, the MCPTT client shall interact with the media plane as specified in 3GPP TS 24.380 [5].

6.2.5.2 Pre-established session case

When the MCPTT client wants to release an MCPTT session using a pre-established session, the MCPTT client:

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

2) shall generate an initial SIP REFER request outside a dialog in accordance with the procedures specified in 3GPP TS 24.229 [4], IETF RFC 4488 [22] and IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27];

3) shall set the Request-URI of the SIP REFER request to the public service identity identifying the pre-established session on the MCPTT server serving the MCPTT user;

4) shall include the Refer-Sub header field with value "false" according to rules and procedures of IETF RFC 4488 [22];

5) shall include the Supported header field with value "norefersub" according to rules and procedures of IETF RFC 4488 [22];

6) shall set the Refer-To header field of the SIP REFER request to the MCPTT session identity to release;

7) shall include the "method" SIP URI parameter with the value "BYE" in the URI in the Refer-To header field;

8) shall include a Target-Dialog header field as specified in IETF RFC 4538 [23] identifying the pre-established session; and

9) shall send the SIP REFER request according to 3GPP TS 24.229 [4].

Upon receiving a SIP 2xx response to the SIP REFER request, the MCPTT client shall interact with media plane as specified in 3GPP TS 24.380 [5].

6.2.6 Receiving an MCPTT session release request

Upon receiving a SIP BYE request, the MCPTT client:

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

2) shall send SIP 200 (OK) response towards MCPTT server according to 3GPP TS 24.229 [4].

6.2.7 Void

6.2.8 Priority call conditions

6.2.8.0 General

The subclauses of the parent subclause contain common procedures to be used for MCPTT emergency group calls and MCPTT imminent peril group calls.

6.2.8.1 MCPTT emergency group call conditions

6.2.8.1.1 SIP INVITE request or SIP REFER request for originating MCPTT emergency group calls

This subclause is referenced from other procedures.

When the MCPTT emergency state is set and the MCPTT user is authorised to initiate an MCPTT emergency group call on the targeted MCPTT group as determined by the procedures of subclause 6.2.8.1.8, the MCPTT client:

1) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body in the SIP INVITE request or SIP REFER request, an <emergency-ind> element set to "true" and if the MCPTT emergency group call state is set to "MEGC 1: emergency-gc-capable", shall set the MCPTT emergency group call state to "MEGC 2: emergency-call-requested";

2) if the MCPTT user has also requested an MCPTT emergency alert to be sent and this is an authorised request for MCPTT emergency alert as determined by the procedures of subclause 6.2.8.1.6, and the MCPTT emergency alert state is set to "MEA 1: no-alert", shall:

   a) set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to "true" and set the MCPTT emergency alert state to "MEA 2: emergency-alert-confirm-pending"; and

   b) include in the SIP INVITE request the specific location information for MCPTT emergency alert as specified in subclause 6.2.9.1;

3) if the MCPTT user has not requested an MCPTT emergency alert to be sent and the MCPTT emergency alert state is set to "MEA 1: no-alert", shall set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to "false"; and

4) if the MCPTT client emergency group state of the group is set to a value other than "MEG 2: in-progress" set the MCPTT client emergency group state of the MCPTT group to "MEG 4: confirm-pending".

NOTE 1: This is the case of an MCPTT user already being in the MCPTT emergency state it initiated previously while originating an MCPTT emergency group call or MCPTT emergency alert. All group calls the MCPTT user originates while in MCPTT emergency state will be MCPTT emergency group calls.

When the MCPTT emergency state is clear and the MCPTT emergency group call state is set to "MEGC 1: emergency-gc-capable" and the received SIP request contains an authorised request for MCPTT emergency group call as determined by the procedures of subclause 6.2.8.1.8, the MCPTT client shall set the MCPTT emergency state and perform the following actions:

1) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body in the SIP INVITE request or SIP REFER request an <emergency-ind> element set to "true" and set the MCPTT emergency group call state to "MEGC 2: emergency-call-requested" state;

2) if the MCPTT user has also requested an MCPTT emergency alert to be sent and this is an authorised request for MCPTT emergency alert as determined by the procedures of subclause 6.2.8.1.6, shall:

   a) include in the application/vnd.3gpp.mcptt-info+xml MIME body the <alert-ind> element set to "true" and set the MCPTT emergency alert state to "MEA 2: emergency-alert-confirm-pending"; and

   b) include in the SIP INVITE request the specific location information for MCPTT emergency alert as specified in subclause 6.2.9.1;

3) if the MCPTT user has not requested an MCPTT emergency alert to be sent, shall set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to "false"; and

4) if the MCPTT client emergency group state of the group is set to a value other than "MEG 2: in-progress" shall set the MCPTT client emergency group state of the MCPTT group to "MEG 4: confirm-pending".

NOTE 2: This is the case of an initial MCPTT emergency group call and optionally an MCPTT emergency alert being sent. As the MCPTT emergency state is not sent, there is no MCPTT emergency alert outstanding.

NOTE 3: An MCPTT group call originated by an affiliated member of an MCPTT group which is in an in-progress emergency state (as tracked on the MCPTT client by the MCPTT client emergency group state) but is not in an MCPTT emergency state of their own will also be an MCPTT emergency group call. The <emergency-ind> and <alert-ind> elements of the application/vnd.3gpp.mcptt-info+xml MIME body do not need to be included in this case and hence no action needs to be taken in this subclause.

6.2.8.1.2 Resource-Priority header field for MCPTT emergency group calls

This subclause is referenced from other procedures.

If the MCPTT emergency group call state is set to either "MEGC 2: emergency-call-requested" or "MEGC 3: emergency-call-granted" and this is an authorised request for an MCPTT emergency group call as determined by the procedures of subclause 6.2.8.1.8, or the MCPTT client emergency group state of the group is set to "MEG 2: in-progress", the MCPTT client shall include in the SIP INVITE request or SIP REFER request a Resource-Priority header field populated with the values for an MCPTT emergency group call as specified in subclause 6.2.8.1.15.

NOTE: The MCPTT client ideally would not need to maintain knowledge of the in-progress emergency state of the group (as tracked on the MCPTT client by the MCPTT client emergency group state) but can use this knowledge to provide a Resource-Priority header field set to emergency level priority, which starts the infrastructure priority adjustment process sooner than otherwise would be the case.

If this is an authorised request to cancel the MCPTT emergency group call as determined by the procedures of subclause 6.2.8.1.7, and the MCPTT client emergency group state of the group is "no-emergency" or "cancel-pending", the MCPTT client shall include in the SIP INVITE request or SIP REFER request a Resource-Priority header field populated with the values for a normal MCPTT group call as specified in subclause 6.2.8.1.15.

6.2.8.1.3 SIP re-INVITE request for cancelling MCPTT in-progress emergency group state

This subclause is referenced from other procedures.

If the MCPTT emergency group call state is set to "MEGC 3: emergency-call-granted" and the MCPTT emergency alert state is set to "MEA 1: no-alert", the MCPTT client shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] with the clarifications given below.

NOTE 1: This procedure assumes that the calling procedure has verified that the MCPTT user has made an authorised request for cancelling MCPTT in-progress emergency group state of the group.

The MCPTT client:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in clause F.1 with the <emergency-ind> element set to "false";

2) shall clear the MCPTT emergency state; and

3) shall set MCPTT emergency group state of the MCPTT group to "MEG 3: cancel-pending"

NOTE 2: This is the case of an MCPTT user who has initiated an MCPTT emergency group call and wants to cancel it.

If the MCPTT emergency group call state is set to "MEGC 3: emergency-call-granted" and the MCPTT emergency alert state is set to a value other than "MEA 1: no-alert" and the MCPTT user has indicated only the MCPTT emergency group call should be cancelled, the MCPTT client:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in clause F.1 with the <emergency-ind> element set to "false"; and

2) shall set the MCPTT emergency group state of the MCPTT group to "MEG 3: cancel-pending".

NOTE 3: This is the case of an MCPTT user has initiated both an MCPTT emergency group call and an MCPTT emergency alert and wishes to only cancel the MCPTT emergency group call. This leaves the MCPTT emergency state set.

If the MCPTT emergency group call state is set to "MEGC 3: emergency-call-granted" and the MCPTT emergency alert state is set to a value other than "MEA 1: no-alert" and the MCPTT user has indicated that the MCPTT emergency alert on the MCPTT group should be cancelled in addition to the MCPTT emergency group call, the MCPTT client:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in clause F.1 with the <emergency-ind> element set to "false";

2) shall if this is an authorised request to cancel an MCPTT emergency alert as determined by the procedures of subclause 6.2.8.1.6:

   a) include in the application/vnd.3gpp.mcptt-info+xml MIME body an <alert-ind> element set to "false";

   b) set the MCPTT emergency alert state to "MEA 4: Emergency-alert-cancel-pending"; and

   c) clear the MCPTT emergency state;

3) should, if this is not an authorised request to cancel an MCPTT emergency alert as determined by the procedures of subclause 6.2.8.1.6, indicate to the MCPTT user that they are not authorised to cancel the MCPTT emergency alert; and

4) shall set the MCPTT emergency group state of the MCPTT group to "MEG 3: cancel-pending".

NOTE 4: This is the case of an MCPTT user that has initiated both an MCPTT emergency group call and an MCPTT emergency alert and wishes to cancel both.

6.2.8.1.4 Receiving a SIP 2xx response to a SIP request for a priority call

In the procedures in this subclause, a priority group call refers to an MCPTT emergency group call or an MCPTT imminent peril group call.

On receiving a SIP 2xx response to a SIP request for a priority group call, the MCPTT client:

1) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested" or "MEGC 3: emergency-call-granted":

   a) shall set the MCPTT client emergency group state of the group to "MEG 2: in-progress" if it was not already set;

   b) if the MCPTT emergency alert state is set to "MEA 2: emergency-alert-confirm-pending" and the SIP 2xx response to the SIP request for a priority group call does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated;

   c) shall set the MCPTT emergency group call state to "MEGC 3: emergency-call-granted"; and

   d) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-capable" and the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; or

2) if the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted" and the SIP 2xx response to the SIP request for an imminent peril group call does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149":

   a) set the MCPTT imminent peril group call state to "MIGC 3: imminent-peril-call-granted"; and

   b) set the MCPTT imminent peril group state to "MIG 2: in-progress".

6.2.8.1.5 Receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to a SIP request for a priority group call

In the procedures in this subclause, a priority group call refers to an MCPTT emergency group call or an MCPTT imminent peril group call.

Upon receiving a SIP 4xx response, SIP 5xx response or a SIP 6xx response to a SIP request for a priority group call the MCPTT client:

1) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested" or "MEGC 3: emergency-call-granted":

   a) shall set the MCPTT emergency group call state to "MEGC 1: emergency-gc-capable";

   b) if the MCPTT client emergency group state of the group is "MEG 4: confirm-pending" shall set the MCPTT client emergency group state of the group to "MEG 1: no-emergency"; and

   c) if the sent SIP request for a priority group call contained an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to a value of "true", shall set the MCPTT emergency alert state to "MEA 1: "no-alert"; and

2) if the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted":

   a) shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; and

   b) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-gc-capable".

6.2.8.1.6 Determining authorisation for initiating or cancelling an MCPTT emergency alert

If the MCPTT client receives a request from the MCPTT user to send an MCPTT emergency alert and:

1) if the <allow-activate-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling MCPTT user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true"; and

2) if the "entry-info" attribute of the <entry> element of the <EmergencyAlert> element contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of:

   a) "DedicatedGroup", and if the <uri-entry> element of the <entry> element of the <EmergencyAlert> element of the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) contains the MCPTT group identity of the MCPTT group targeted by the calling MCPTT user; or

   b) "UseCurrentlySelectedGroup" and the <allow-MCPTT-emergency-alert> element of the <list-element> of the group document identified by the MCPTT group identity targeted for the emergency alert is set to a value of "true" as specified in 3GPP TS 24.481 [31];

then the MCPTT emergency alert request shall be considered to be an authorised request for an MCPTT emergency alert. In all other cases, it shall be considered to be an unauthorised request for an MCPTT emergency alert.

If the MCPTT client receives a request from the MCPTT user to cancel an MCPTT emergency alert to an MCPTT group, and if the <allow-cancel-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling MCPTT user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true", then the MCPTT emergency alert cancellation request shall be considered to be an authorised request to cancel an MCPTT emergency alert. In all other cases, it shall be considered to be an unauthorised request to cancel an MCPTT emergency alert.

6.2.8.1.7 Determining authorisation for cancelling the in-progress emergency state of an MCPTT group

When the MCPTT client receives a request from the MCPTT user to cancel the in-progress emergency state of a group the MCPTT client and:

1) if the <allow-cancel-group-emergency> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling MCPTT user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true", then the in-progress emergency group state cancel request shall be considered to be an authorised request for in-progress emergency group state cancellation; or

2) if the <allow-cancel-group-emergency> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling MCPTT user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "false", then the in-progress emergency group state cancel request shall be considered to be an unauthorised request for in-progress emergency group state cancellation.

6.2.8.1.8 Determining authorisation for originating a priority group call

When the MCPTT client receives a request from the MCPTT user to originate an MCPTT emergency group call the MCPTT client shall check the following:

1) if the <allow-emergency-group-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true" and

   a) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> element contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "DedicatedGroup" and if the <uri-entry> element of the <entry> element of the <MCPTTGroupInitiation> element contains the identity of the MCPTT group targeted by the calling MCPTT user; or

   b) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UseCurrentlySelectedGroup";

   then the MCPTT emergency group call request shall be considered to be an authorised request for an MCPTT emergency group call;

In all other cases, the request to originate an MCPTT emergency group call shall be considered to be an unauthorised request to originate an MCPTT emergency group call.

When the MCPTT client receives a request from the MCPTT user to originate an MCPTT imminent peril group call the MCPTT client shall check the following:

1 if the <allow-imminent-peril-call> element of <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true" and:

   a) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element contained within the <ImminentPerilCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "DedicatedGroup" and if the <MCPTTGroupInitiation> element contains the identity of the MCPTT group targeted by the calling MCPTT user; or

   b) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element contained within the <ImminentPerilCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UseCurrentlySelectedGroup";

   then the MCPTT imminent peril group call request shall be considered to be an authorised request for an MCPTT imminent peril group call;

In all other cases, the request to originate an MCPTT imminent peril group call shall be considered to be an unauthorised request to originate an MCPTT imminent peril group call.

6.2.8.1.9 SIP request for originating MCPTT imminent peril group calls

This subclause is referenced from other procedures.

When the MCPTT client receives a request from the MCPTT user to originate an MCPTT imminent peril group call, and this is an authorised request for an MCPTT imminent peril group call as determined by the procedures of subclause 6.2.8.1.8, the MCPTT client:

1) if the MCPTT client imminent peril group state is set to "MIGC 1: imminent-peril-gc-capable" and the in-progress emergency state of the group is set to a value of "false":

   a) shall include in the SIP request a MIME mcpttinfo body as defined in Annex F.1 with the <imminentperil-ind> element set to "true" and set the MCPTT emergency group call state to "MIGC 2: imminent-peril-call-requested" state; and

   b) if the MCPTT client imminent peril group state of the group is set to a value other than "MIG 2: in-progress" shall set the MCPTT client emergency group state of the MCPTT group to "MIG 4: confirm-pending".

NOTE: An MCPTT group call originated by an affiliated member of an MCPTT group which is in an in-progress imminent peril state (as tracked on the MCPTT client by the MCPTT client imminent peril group state) will also have the priority associated with MCPTT imminent peril group calls. The <imminentperil-ind> element of the MIME mcpttinfo body does not need to be included in this case, nor do any state changes result and hence no action needs to be taken in this subclause.

6.2.8.1.10 Determining authorisation for cancelling an imminent peril group call

When the MCPTT client receives a request from the MCPTT user to cancel an MCPTT imminent peril group call the MCPTT client shall:

1) if the <allow-cancel-imminent-peril> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true" the MCPTT imminent peril call cancellation request shall be considered to be an authorised request to cancel the MCPTT imminent peril group call; or

2) if the <allow-cancel-imminent-peril> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "false" the MCPTT imminent peril call cancellation request shall be considered to be an unauthorised request to cancel the MCPTT imminent peril group call.

6.2.8.1.11 SIP re-INVITE request for cancelling MCPTT in-progress imminent peril group state

This subclause is referenced from other procedures.

If the MCPTT imminent peril group call state is set to "MIGC 3: imminent-peril-call-granted" or the MCPTT imminent peril group state of the MCPTT group is set to "MIG 2: in-progress", the MCPTT client shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] with the clarifications given below.

NOTE 1: This procedure assumes that the calling procedure has verified that the MCPTT user has made an authorised request for cancelling the in-progress imminent peril group state of the group.

The MCPTT client:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in clause F.1 with the <imminentperil-ind> element set to "false"; and

2) shall set MCPTT imminent peril group state of the MCPTT group to "MIG 3: cancel-pending".

NOTE 2: This is the case of an MCPTT user who has initiated an MCPTT imminent peril group call and wants to cancel it, or another authorised member of the group who wishes to cancel the in-progress imminent peril state of the group.

6.2.8.1.12 Resource-Priority header field for MCPTT imminent peril group calls

This subclause is referenced from other procedures.

When the MCPTT imminent peril group call state is set "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted" and the MCPTT user is authorised to initiate an MCPTT imminent peril group call on the targeted MCPTT group as determined by the procedures of subclause 6.2.8.1.8, or the MCPTT client imminent peril state of the group is set to "MIG 2: in-progress", the MCPTT client:

1) shall include in the SIP INVITE request or SIP REFER request a Resource-Priority header field populated with the values for an MCPTT imminent peril group call as specified in subclause 6.2.8.1.15.

NOTE: The MCPTT client ideally would not need to maintain knowledge of the in-progress imminent peril state of the group (as tracked on the MCPTT client by the MCPTT client imminent peril group state) but can use this knowledge to provide a Resource-Priority header field set to imminent peril level priority, which starts the infrastructure priority adjustment process sooner than otherwise would be the case.

When the MCPTT imminent peril group call state is set to "MIGC 1: imminent-peril-gc-capable" and the MCPTT user is authorised to cancel MCPTT imminent peril group calls as determined by the procedures of subclause 6.2.8.1.10, or the MCPTT client imminent peril group state of the group is "MIG 1: no-imminent-peril" or "MIG 3: cancel-pending", the MCPTT client:

1) shall include in the SIP INVITE request or SIP REFER request a Resource-Priority header field populated with the values for a normal MCPTT group call as specified in subclause 6.2.8.1.15.

6.2.8.1.13 Receiving a SIP INFO request in the dialog of a SIP request for a priority group call

This subclause is referenced from other procedures.

Upon receiving a SIP INFO request within the dialog of the SIP request for a priority group call:

- with the Info-Package header field containing the g.3gpp.mcptt-info package name;

- with the application/vnd.3gpp.mcptt-info+xml MIME body associated with the info package according to IETF RFC 6086 [54]; and

- with one or more of the <alert-ind>, <imminentperil-ind> and <emergency-ind> elements set in the application/vnd.3gpp.mcptt-info+xml MIME body;

the MCPTT client:

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

2) if the MCPTT emergency group call state is set to "MEGC 3: emergency-call-granted":

   a) if the MCPTT emergency alert state is set to "MEA 2: emergency-alert-confirm-pending":

      i) if the <alert-ind> element is set to a value of "false", shall set the MCPTT emergency alert state to "MEA 1: no-alert"; and

      ii) if the <alert-ind> element is set to a value of "true", shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated";

3) if the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted":

   a) if the <imminentperil-ind> element is set to a value of "false" and an <emergency-ind> element is set to a value of "true", shall:

      i) set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril";

      ii) set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-capable"; and

      iii) set the MCPTT client emergency group state of the group to "MEG 2: in-progress"; and

NOTE 1: This is the case of an MCPTT client attempting to make an imminent peril group call when the group is in an in-progress emergency group state. The MCPTT client will then receive a notification that the imminent peril call request was denied, however they will be participating at the emergency level priority of the group. This could occur for example when an MCPTT client requests an imminent peril call to a group that they are not currently affiliated with.

NOTE 2: the MCPTT client emergency group state above is the MCPTT client's view of the in-progress emergency state of the group.

4) if the SIP request for a priority group call sent by the MCPTT client did not contain an <originated-by> element and if the MCPTT emergency alert state is set to "MEA 4: Emergency-alert-cancel-pending":

   a) if the <alert-ind> element contained in the SIP INFO request is set to a value of "true", shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated"; and

   b) if the <alert-ind> element contained in the SIP INFO request is set to a value of "false", shall set the MCPTT emergency alert state to "MEA 1: no-alert".

6.2.8.1.14 SIP re-INVITE request for cancelling the in-progress emergency group state of a group by a third-party

This subclause is referenced from other procedures.

Upon receiving an authorised request to cancel an in-progress emergency group state of a group as determined by the procedures of subclause 6.2.8.1.7 from an MCPTT user, the MCPTT client shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] with the clarifications given below.

The MCPTT client:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in clause F.1 with the <emergency-ind> element set to "false";

2) shall set MCPTT emergency group state of the MCPTT group to "MEG 3: cancel-pending"; and

3) if the MCPTT user has indicated that an MCPTT emergency alert on the MCPTT group originated by another MCPTT user should be cancelled and this is an authorised request for an MCPTT emergency alert cancellation as determined by the procedures of subclause 6.2.8.1.6:

   a) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <alert-ind> element set a value of "false"; and

b) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <originated-by> element set to the MCPTT ID of the MCPTT user who originated the MCPTT emergency alert.

NOTE: When an MCPTT emergency alert is cancelled by a MCPTT user other than its originator, the <originated-by> element is needed to identify which MCPTT emergency alert is being cancelled, as more than one MCPTT user could have originated emergency alerts to the same group.

6.2.8.1.15 Retrieving Resource-Priority header field values

This subclause is referenced from other procedures.

When determining the Resource-Priority header field namespace and priority values as specified in IETF RFC 8101 [48] for an MCPTT emergency group call or MCPTT emergency private call the MCPTT client:

1) shall retrieve the value of the <resource-priority-namespace> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]); and

2) shall retrieve the value of the <resource-priority-priority> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]).

When determining the Resource-Priority header field namespace and priority values as specified in IETF RFC 8101 [48] for an MCPTT imminent peril group call the MCPTT client:

1) shall retrieve the value of the <resource-priority-namespace> element contained in the <imminent-peril-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]); and

2) shall retrieve the value of the <resource-priority-priority> element contained in the <imminent-peril-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]).

When determining the Resource-Priority header field namespace and priority values as specified in IETF RFC 8101 [48] for a normal MCPTT group or private call the MCPTT client:

1) shall retrieve the value of the <resource-priority-namespace> element contained in the <normal-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]); and

2) shall retrieve the value of the <resource-priority-priority> element contained in the <normal-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]).

NOTE: The "normal" Resource-Priority header field value is needed to return to a normal priority value from a priority value adjusted for an MCPTT emergency group or private call or an MCPTT imminent peril group call. The "normal" priority received from the EPS by use of the "normal" Resource-Priority header field value is expected to be the same as the "normal" priority received from the EPS when initiating a call with no Resource-Priority header field included.

6.2.8.1.16 Handling receipt of a SIP re-INVITE request for priority group call origination status within a pre-established session

This subclause is referenced from other procedures.

Upon receipt of a SIP re-INVITE request within the pre-established session targeted by the sent SIP REFER request, and if the sent SIP REFER request was a request for an MCPTT emergency group call or an MCPTT imminent peril group call, the MCPTT client:

1) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested":

a) if there is no <emergency-ind> element or an <emergency-ind> element set to a value of "true" contained in the application/vnd.3gpp.mcptt-info+xml MIME body received in the SIP re-INVITE request, and if no <imminentperil-ind> element is included:

i) shall set the MCPTT client emergency group state of the group to "MEG 2: in-progress" if it was not already set; and

ii) shall set the MCPTT emergency group call state to "MEGC 3: emergency-call-granted"; and

b) if the MCPTT emergency alert state is set to "MEA 2: emergency-alert-confirm-pending":

i) if the SIP re-INVITE request contains an <alert-ind> element set to a value of "true" or does not contain an <alert-ind> element, shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated"; or

ii) if the SIP re-INVITE request contains an <alert-ind> element set to a value of "false", shall set the MCPTT emergency alert state to "MEA 1: no-alert"; and

2) if the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested:

a) if the sip re-INVITE request contains an <imminentperil-ind> element set to a value of "true" or does not contain an <imminentperil-ind> element, shall:

i) set the MCPTT imminent peril group call state to "MIGC 3: imminent-peril-call-granted"; and

ii) set the MCPTT imminent peril group state to "MIG 2: in-progress"; or

b) if the SIP re-INVITE request contains <imminentperil-ind> element set to a value of "false" and an <emergency-ind> element set to a value of "true", shall set the MCPTT client emergency group state of the group to "MEG 2: in-progress".

NOTE: This is the case of an MCPTT client attempting to make an imminent peril group call when the group is in an in-progress emergency group state. The MCPTT client will then receive a notification that the imminent peril call request was denied, however they will be participating at the emergency level priority of the group. This could occur for example when an MCPTT client requests an imminent peril call to a group that they are not currently affiliated with.

6.2.8.1.17 Priority group call conditions upon receiving call release

This subclause is referenced from other procedures.

Upon receiving a request to release the MCPTT emergency group call or an MCPTT imminent peril group call in an MCPTT group session is in-progress or is in the process of being established:

1) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested":

a) shall set the MCPTT emergency group call state to "MEGC 1: emergency-gc-capable";

b) if the MCPTT client emergency group state of the group is "MEG 3: confirm-pending" shall set the MCPTT client emergency group state of the group to "MEG 1: no-emergency"; and

c) if the MCPTT emergency alert state is set to "MEA 2: emergency-alert-confirm-pending" shall set the MCPTT emergency alert state to "MEA 1: "no-alert"; and

2) if the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested":

a) if the MCPTT imminent peril group call state of the group is "MIG 3: confirm-pending", shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; and

b) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-capable".

NOTE: The above conditions can be applied upon a call being released within a pre-established by the procedures specified in subclause 9.2.2 in 3GPP TS 24.380 [5].

6.2.8.1.18 Emergency private call conditions upon receiving call release

This subclause is referenced from other procedures.

Upon receiving a request to release the MCPTT session when an MCPTT emergency private call is in-progress or is in the process of being established:

1) if the MCPTT emergency private call state is set to "MEPC 2: emergency-call-requested":

   a) shall set the MCPTT emergency private call state to "MEPC 1: emergency-pc-capable";

   b) if the MCPTT emergency private priority state of the private call is "MEPP 3: confirm-pending" shall set the MCPTT emergency private priority state of the private call to "MEPP 1: no-emergency"; and

   c) if the MCPTT private emergency alert state is set to "MPEA 2: emergency-alert-confirm-pending shall set the MCPTT private emergency alert state to "MPEA 1: no-alert".

NOTE: The above conditions can be applied upon a call being released within a pre-established by the procedures specified in subclause 9.2.2 of 3GPP TS 24.380 [5].

6.2.8.2 Request for an originating broadcast group call

NOTE: This subclause is referenced from other procedures.

When the MCPTT user initiates a broadcast group call, the MCPTT client:

1) in the case of the prearranged group call is initiated on-demand, shall include in the application/vnd.3gpp.mcptt-info+xml MIME body the <broadcast-ind> element set to "true" as defined in clause F.1; and

2) in the case the prearranged group call is initiated using a pre-established session, shall include in the application/vnd.3gpp.mcptt-info+xml MIME body in the "body" URI header field in the Refer-To header field the <broadcast-ind> element set to "true" as defined in clause F.1.

6.2.8.3 MCPTT emergency private call conditions

6.2.8.3.1 Authorisations

6.2.8.3.1.1 Determining authorisation for initiating an MCPTT emergency private call

If the MCPTT client receives a request from the MCPTT user to originate an MCPTT emergency private call and:

1) if the <allow-emergency-private-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true"; and

   a) if the "entry-info" attribute of the <entry> element of the <MCPTTPrivateRecipient> element of the <EmergencyCall> element contained within the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UsePreConfigured" and if the <uri-entry> element of the <entry> element of the <MCPTTPrivateRecipient> element contains the MCPTT ID of the MCPTT user targeted by the calling MCPTT user; or

   b) if the "entry-info" attribute of the <entry> element of the <MCPTTPrivateRecipient> element of the <EmergencyCall> element contained within the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "LocallyDetermined";

then the MCPTT client shall consider the MCPTT emergency private call request to be an authorised request for an MCPTT emergency private call. In all other cases the MCPTT client shall consider the MCPTT emergency private call request to be an unauthorised request for an MCPTT emergency private call.

6.2.8.3.1.2 Determining authorisation for cancelling an MCPTT emergency private call

If the MCPTT client receives a request from the MCPTT user to cancel an MCPTT emergency private call and if the <allow-cancel-private-emergency-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true", then the MCPTT emergency private call cancellation request shall be considered to be an authorised request for an MCPTT emergency private call cancellation.

In all other cases, the MCPTT emergency private call cancellation request shall be considered to be an unauthorised request for an MCPTT emergency private call cancellation.

6.2.8.3.1.3 Determining authorisation for initiating or cancelling an MCPTT emergency alert to a MCPTT user

If the MCPTT client receives a request from the MCPTT user to send an MCPTT emergency alert to an MCPTT user and:

1) if the <allow-activate-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling MCPTT user as specified in 3GPP TS 24.484 [50] is set to a value of "true"; and

2) if the "entry-info" attribute of the <entry> element of the <PrivateEmergencyAlert> element contained within the <OnNetwork> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of:

   a) "UsePreConfigured", and if the <uri-entry> element of the <entry> element of the <PrivateEmergencyAlert> element of the <OnNetwork> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) contains the MCPTT ID of the targeted MCPTT user; or

   b) "LocallyDetermined";

then the MCPTT emergency alert request shall be considered to be an authorised request for an MCPTT emergency alert. In all other cases, it shall be considered to be an unauthorised request for an MCPTT emergency alert.

If the MCPTT client receives a request from the MCPTT user to cancel an MCPTT emergency alert to an MCPTT user, and if the <allow-cancel-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling MCPTT user as specified in 3GPP TS 24.484 [50] is set to a value of "true", then the MCPTT emergency alert cancellation request shall be considered to be an authorised request to cancel an MCPTT emergency alert. In all other cases, it shall be considered to be an unauthorised request to cancel an MCPTT emergency alert.

6.2.8.3.2 SIP request for originating MCPTT emergency private calls

This subclause is referenced from other procedures.

When the MCPTT emergency private call state is set to "MEPC 1: emergency-pc-capable" and this is an authorised request for an MCPTT emergency private call as determined by the procedures of subclause 6.2.8.3.1.1, the MCPTT client:

1) shall set the MCPTT emergency state if not already set;

2) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body in the SIP request an <emergency-ind> element set to "true" and set the MCPTT emergency private call state to "MEPC 2: emergency-pc-requested";

3) if the MCPTT user has also requested an MCPTT emergency alert to be sent and this is an authorised request for MCPTT emergency alert as determined by the procedures of subclause 6.2.8.3.1.3, shall:

   a) include in the application/vnd.3gpp.mcptt-info+xml MIME body the <alert-ind> element set to "true" and set the MCPTT private emergency alert state to "MPEA 2: emergency-alert-confirm-pending"; and

   b) include in the SIP request the specific location information for MCPTT emergency alert as specified in subclause 6.2.9.1;

4) if the MCPTT user has not requested an MCPTT emergency alert to be sent, shall set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to "false"; and

5) if the MCPTT emergency private priority state of this private call is set to a value other than "MEPP 2: in-progress" shall set the MCPTT emergency private priority state to "MEPP 3: confirm-pending".

6.2.8.3.3 Resource-Priority header field for MCPTT emergency private calls

This subclause is referenced from other procedures.

If the MCPTT emergency private call state is set to either "MEPC 2: emergency-pc-requested" or "MEPC 3: emergency-pc-granted" and this is an authorised request for an MCPTT emergency private call as determined by the procedures of subclause 6.2.8.3.1.1, or the MCPTT emergency private priority state of the call is set to "MEPP 2: in-

progress", the MCPTT client shall include in the SIP request a Resource-Priority header field populated with the values for an MCPTT emergency private call as specified in subclause 6.2.8.1.15.

NOTE: The MCPTT client ideally would not need to maintain knowledge of the in-progress emergency state of the call (as tracked on the MCPTT client by the MCPTT client emergency private state) but can use this knowledge to provide a Resource-Priority header field set to emergency level priority, which starts the infrastructure priority adjustment process sooner than otherwise would be the case.

If this is an authorised request to cancel the MCPTT emergency private call as determined by the procedures of subclause 6.2.8.3.1.2, or the MCPTT emergency private priority state of the private call is "MEPP 1: no-emergency" or "MEPP 3: cancel-pending", the MCPTT client shall include in the SIP request a Resource-Priority header field populated with the values for a normal MCPTT private call as specified in subclause 6.2.8.1.15.

6.2.8.3.4 Receiving a SIP 2xx response to a SIP request for an MCPTT emergency private call

This subclause is referenced from other procedures.

On receiving a SIP 2xx response to a SIP request for an MCPTT emergency private call and if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested" or "MEPC 3: emergency-pc-granted", the MCPTT client:

1) shall set the MCPTT emergency private priority state of the call to "MEPP 2: in-progress" if it was not already set;

2) shall set the MCPTT emergency private call state to "MEPC 3: emergency-pc-granted"; and

3) if the MCPTT private emergency alert state is set to "MPEA 2: emergency-alert-confirm-pending" and the SIP 2xx response to the SIP request for a priority private call does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", shall set the MCPTT private emergency alert state to "MPEA 3: emergency-alert-initiated".

6.2.8.3.5 Receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to a SIP request for an MCPTT emergency private call

Upon receiving a SIP 4xx response, SIP 5xx response or a SIP 6xx response to a SIP request for an MCPTT emergency private call and if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested" or "MEPC 3: emergency-pc-granted", the MCPTT client:

1) shall set the MCPTT emergency private call state to "MEPC 1: emergency-pc-capable";

2) if the MCPTT emergency private priority state of the private call is "MEPP 3: confirm-pending" shall set the MCPTT emergency private priority state of the private call to "MEPP 1: no-emergency"; and

3) if the sent SIP request for an MCPTT emergency private call contained an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to a value of "true", shall set the MCPTT private emergency alert state to "MPEA 1: no-alert".

6.2.8.3.6 SIP re-INVITE request for cancelling MCPTT emergency private call state

This subclause is referenced from other procedures.

When the MCPTT emergency private call state is set to "MEPC 3: emergency-pc-granted" and the MCPTT emergency alert state is set to "MPEA 1: no-alert", the MCPTT client shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] with the clarifications given below.

NOTE 1: This procedure assumes that the MCPTT client in the calling procedure has verified that the MCPTT user has made an authorised request for cancelling MCPTT the in-progress emergency private call state of the call.

The MCPTT client:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in clause F.1 with the <emergency-ind> element set to "false";

2) shall clear the MCPTT emergency state; and

3) shall set MCPTT emergency private priority state of the MCPTT emergency private call to "MEPP 3: cancel-pending".

NOTE 2: This is the case of an MCPTT user who has initiated an MCPTT emergency private call and wants to cancel it.

When the MCPTT emergency private call state is set to "MEPPC 3: emergency-pc-granted" and the MCPTT emergency alert state is set to a value other than "MPEA 1: no-alert" and the MCPTT user has indicated only the MCPTT emergency private call should be cancelled, the MCPTT client:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in clause F.1 with the <emergency-ind> element set to "false"; and

2) shall set the MCPTT emergency private priority state of the MCPTT emergency private call to "MEPP 3: cancel-pending";

NOTE 3: This is the case of an MCPTT user has initiated both an MCPTT emergency private call and an MCPTT emergency alert and wishes to only cancel the MCPTT emergency private call. This leaves the MCPTT emergency state set.

When the MCPTT emergency private call state is set to "MEPC 3: emergency-pc-granted" and the MCPTT emergency alert state is set to a value other than "MPEA 1: no-alert" and the MCPTT user has indicated that the MCPTT emergency alert on the MCPTT private call should be cancelled in addition to the MCPTT emergency private call, the MCPTT client:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in annex F.1 with the <emergency-ind> element set to "false";

2) shall, if this is an authorised request to cancel an MCPTT emergency alert as determined by the procedures of subclause 6.2.8.3.1.3:

   a) include in the application/vnd.3gpp.mcptt-info+xml MIME body an <alert-ind> element set to "false"; and

   b) set the MCPTT private emergency alert state to "MPEA 4: emergency-alert-cancel-pending";

3) if this is not an authorised request to cancel an MCPTT emergency alert as determined by the procedures of subclause 6.2.8.3.1.3, should indicate to the MCPTT user they are not authorised to cancel the MCPTT emergency alert;

4) shall set the MCPTT emergency private priority state of the MCPTT to "MEPP 3: cancel-pending"; and

5) shall clear the MCPTT emergency state.

NOTE 4: This is the case of an MCPTT user that has initiated both an MCPTT emergency private call and an MCPTT emergency alert and wishes to cancel both.

6.2.8.3.7 Receiving a SIP INFO request in the dialog of a SIP request for a priority private call

This subclause is referenced from other procedures.

Upon receiving a SIP INFO request within the dialog of the SIP request for a priority private call:

- with the Info-Package header field containing the g.3gpp.mcptt-info package name;

- with the application/vnd.3gpp.mcptt-info+xml MIME body associated with the info package according to IETF RFC 6086 [54]; and

- with one or more of the <alert-ind>, <imminentperil-ind> and <emergency-ind> elements set in the application/vnd.3gpp.mcptt-info+xml MIME body;

the MCPTT client:

1) if the MCPTT private emergency alert state is set to "MPEA 2: emergency-alert-confirm-pending":

a) if the <alert-ind> element is set to a value of "false", shall set the MCPTT private emergency alert state to "MPEA 1: no-alert"; and

b) if the <alert-ind> element set to a value of "true", shall set the MCPTT private emergency alert state to "MPEA 3: emergency-alert-initiated"; and

2) if the MCPTT private emergency alert state is set to "MPEA 4: Emergency-alert-cancel-pending":

a) if the <alert-ind> element is set to a value of "true", shall set the MCPTT private emergency alert state to "MPEA 3: emergency-alert-initiated"; and

b) if the <alert-ind> element is set to a value of "false", shall set the MCPTT private emergency alert state to "MPEA 1: no-alert".

6.2.8.3.8 SIP re-INVITE request for cancelling the MCPTT emergency private call state by a third-party

This subclause is referenced from other procedures.

Upon receiving a request to cancel the MCPTT emergency private call state from an MCPTT user other than the originator of the MCPTT emergency private call, the MCPTT client shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] with the clarifications given below.

The MCPTT client:

NOTE 1: This procedure assumes that the calling procedure has verified that the MCPTT user has made an authorised request for cancelling the MCPTT emergency private call state of the call.

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in clause F.1 with the <emergency-ind> element set to "false";

2) shall set the MCPTT emergency private priority state of the MCPTT emergency private call to "MEPP 3: cancel-pending"; and

3) if the MCPTT user has indicated that an MCPTT emergency alert associated with the MCPTT emergency private call originated by another MCPTT user should be cancelled and this is an authorised request for an MCPTT emergency alert cancellation as determined by the procedures of subclause 6.2.8.3.1.3:

a) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <alert-ind> element set to a value of "false"; and

b) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <originated-by> element set to the MCPTT ID of the MCPTT user who originated the MCPTT emergency alert.

NOTE 2: When an MCPTT emergency alert is cancelled by a MCPTT user other than its originator, the <originated-by> element is needed to identify which MCPTT emergency alert is being cancelled, as conceivably each participant in the MCPTT emergency private call could have originated an MCPTT emergency alert.

6.2.8.3.9 Retrieving a KMS URI associated with an MCPTT ID

If the MCPTT client needs to retrieve a KMS URI associated to an identified MCPTT ID for on network operation, the MCPTT client:

1) shall search for the <entry> element of the <PrivateCallURI> element of the <PrivateCallList> element entry of the <Common> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) containing the identified MCPTT ID;

a) if the identified MCPTT ID is found and if the <entry> element of the <PrivateCallKMSURI> element of the <anyExt> element of the <PrivateCallList> element entry identified is not empty, shall retrieve the KMS URI contained therein; or

b) if the identified MCPTT ID is not found or the <entry> element of the <PrivateCallKMSURI> element is empty, shall retrieve the <kms> element of the <App-Server-Info> element of the <on-network> element of the MCPTT UE

initial configuration document (see the MCPTT UE initial configuration document in 3GPP TS 24.484 [50]) and consider that to be the KMS URI associated with the MCPTT ID.

If the MCPTT client needs to retrieve a KMS URI associated to an identified MCPTT ID for off network operation, the MCPTT client:

1) shall search for /<*x*>/<x>/Common/PrivateCall/UserList/<x>/Entry/MCPTTID leaf node containing the identified MCPTT ID (see the MCPTT user profile MO in 3GPP TS 24.483 [45]);

   a) if the identified MCPTT ID is found:

      i) shall retrieve the /<*x*>/<x>/Common/PrivateCall/UserList/<x>/Entry/PrivateCallKMSURI leaf node (see the MCPTT user profile MO in 3GPP TS 24.483 [45]); and

      ii) if the PrivateCallKMSURI leaf node in the same /<x>/<x>/Common/PrivateCall/UserList/<x>/Entry/ interior node as the MCPTTID leaf node containing the identified MCPTT ID is not empty, shall consider its value to be the KMS URI associated with the MCPTT ID; and

   b) if the identified MCPTT ID is not found or if the /<*x*>/<x>/Common/PrivateCall/UserList/<x>/Entry/PrivateCallKMSURI leaf node is empty:

      i) shall retrieve /<*x*>/OnNetwork/AppServerInfo/KMS leaf node (see the MCPTT UE initial configuration document in 3GPP TS 24.483 [45]); and

      ii) shall consider the value of the /<*x*>/OnNetwork/AppServerInfo/KMS leaf node to be the KMS URI associated with the MCPTT ID.

6.2.9 Location information

6.2.9.1 Location information for location reporting

This procedure is initiated by the MCPTT client when it is including location report information:

1) as part of a SIP request containing an MCPTT emergency alert; or

2) as part of a SIP request for a specified location trigger.

The MCPTT client:

1) if location information is being included as part of a SIP request for a specified location trigger criteria as configured in a <TriggeringCriteria> element contained in a <Configuration> element contained in an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in Annex F.3 as received in a SIP MESSAGE request by the procedures of subclause 13.3.2:

   a) shall include in the SIP request the specific location information as specified by the procedures of subclause 13.3.4.2; and

   b) shall skip the rest of the steps;

2) if location information is being included as part of a SIP request containing an MCPTT emergency alert:

   a) shall include an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in Annex F.3 with a <Report> element included in the <location-info> root element;

   b) shall set the <ReportType> element of the <Report> element to a value of "Emergency";

   c) if the MCPTT client has been configured with an <EmergencyLocationInformation> element contained in a <Configuration> element contained in an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in Annex F.3 and received in a SIP MESSAGE request by the procedures of subclause 13.3.2;

      i) shall populate the <CurrentLocation> element of the <Report> element as indicated by the <EmergencyLocationInformation> element contained in the <Configuration> element contained in an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in Annex F.3 and previously received by the procedures of subclause 13.3.2; and

ii) shall skip the rest of the steps; and

d) if the MCPTT client has not been configured with an <EmergencyLocationInformation> element contained in a <Configuration> element contained in an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in Annex F.3 and received in a SIP MESSAGE request by the procedures of subclause 13.3.2:

i) shall include in the <CurrentLocation> element of the <Report> element of the application/vnd.3gpp.mcptt-location-info+xml MIME body a <CurrentCoordinate> element populated as specified in Annex F.3.3.

NOTE: According to local policy, additional location information elements specified in Annex F.3.3 can be included in the <CurrentLocation> element in the event that no <EmergencyLocationInformation> element was previously received.

6.3 MCPTT server procedures

6.3.1 Distinction of requests sent to the MCPTT server

6.3.1.1 SIP INVITE request

The MCPTT server needs to distinguish between the following initial SIP INVITE requests for originations and terminations:

- SIP INVITE requests routed to the participating MCPTT function as a result of processing initial filter criteria at the S-CSCF in accordance with the origination procedures as specified in 3GPP TS 24.229 [4] with the Request-URI set to a public service identity of the participating MCPTT function that identifies the pre-established session set-up. Such requests are known as "SIP INVITE request for establishing a pre-established session" in the procedures in the present document;

- SIP INVITE requests routed to the participating MCPTT function as a result of processing initial filter criteria at the S-CSCF in accordance with the origination procedures as specified in 3GPP TS 24.229 [4] and the Request-URI is set to a public service identity of the participating MCPTT function that does not identify the pre-established session set-up. Such requests are known as "SIP INVITE request for originating participating MCPTT function" in the procedures in the present document;

- SIP INVITE requests routed to the participating MCPTT function as a result of processing initial filter criteria at the S-CSCF in accordance with the termination procedures as specified in 3GPP TS 24.229 [4] and the Request-URI contains a PSI of the terminating participating MCPTT function. Such requests are known as "SIP INVITE request for terminating participating MCPTT function" in the procedures in the present document;

- SIP INVITE requests routed to the controlling MCPTT function as a result of PSI routing on the originating side in accordance with the originating procedures as specified in 3GPP TS 24.229 [4], or as a result of direct PSI routing, in accordance with the termination procedures as specified in 3GPP TS 24.229 [4], the Request-URI is set to a public service identity for MCPTT private call and the Contact header field does not contain the isfocus media feature tag specified in IETF RFC 3840 [16]. Such requests are known as "SIP INVITE request for controlling MCPTT function of a private call" in the procedures in the present document;

- SIP INVITE requests routed to the controlling MCPTT function as a result of PSI routing on the originating side in accordance with the originating procedures as specified in 3GPP TS 24.229 [4], or as a result of direct PSI routing, in accordance with the termination procedures as specified in 3GPP TS 24.229 [4], the Request-URI is set to a public service identity serving an MCPTT group and the Contact header field does not contain the isfocus media feature tag specified in IETF RFC 3840 [16]. Such requests are known as "SIP INVITE request for controlling MCPTT function of an MCPTT group" in the procedures in the present document;

- SIP INVITE requests routed to the non-controlling MCPTT function of an MCPTT group as a result of direct PSI routing, in accordance with the termination procedures as specified in 3GPP TS 24.229 [4], the Request-URI is set to a public service identity serving an MCPTT group and the Contact header field contains the isfocus media feature tag specified in IETF RFC 3840 [16]; Such requests are known as "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" in the procedures in the present document;

- SIP INVITE requests routed to the controlling MCPTT function as a result of PSI routing on the originating side in accordance with the originating procedures as specified in 3GPP TS 24.229 [4], or as a result of direct PSI

routing, in accordance with the termination procedures as specified in 3GPP TS 24.229 [4], the Request-URI is set to a public service identity for first-to-answer call and the Contact header field does not contain the isfocus media feature tag specified in IETF RFC 3840 [16]. Such requests are known as "SIP INVITE request for controlling MCPTT function of a first-to-answer call" in the procedures in the present document; and

- SIP INVITE requests routed to the controlling MCPTT function as a result of PSI routing on the originating side in accordance with the originating procedures as specified in 3GPP TS 24.229 [4], or as a result of direct PSI routing, in accordance with the termination procedures as specified in 3GPP TS 24.229 [4], the Request-URI is set to a public service identity for MCPTT ambient listening call and the Contact header field does not contain the isfocus media feature tag specified in IETF RFC 3840 [16]. Such requests are known as "SIP INVITE request for controlling MCPTT function of an ambient listening call" in the procedures in the present document.

6.3.1.2 SIP REFER request

The MCPTT server needs to distinguish between the following initial SIP REFER request for originations and terminations:

- SIP REFER requests routed to the participating MCPTT function as a result of processing initial filter criteria at the S-CSCF in accordance with the origination procedures as specified in 3GPP TS 24.229 [4] with the Request-URI set to a public service identity identifying the pre-established session on the participating MCPTT function. Such requests are known as "SIP REFER request for a pre-established session" in the procedures in the present document.

6.3.1.3 SIP MESSAGE request

The MCPTT server needs to distinguish between the following SIP MESSAGE request for originations and terminations:

- SIP MESSAGE requests routed to the participating MCPTT function as a result of processing initial filter criteria at the S-CSCF in accordance with the origination procedures as specified in 3GPP TS 24.229 [4] with the Request-URI set to the MBMS public service identity of the participating MCPTT function. Such requests are known as "SIP MESSAGE request for an MBMS listening status update" in the procedures in the present document;

- SIP MESSAGE request routed to the participating MCPTT function as a result of initial filter criteria containing a Content-Type header field set to "application/vnd.3gpp.mcptt-location-info+xml" and includes an XML body containing a Location root element containing a Report element. Such requests are known as "SIP MESSAGE request for location reporting" in the present document;

- SIP MESSAGE requests routed to the originating participating MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the participating MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element containing a <mcptt-Params> element containing an <emergency-ind> element or an <alert-ind> element. Such requests are known as "SIP MESSAGE requests for emergency notification for originating participating MCPTT function" in the procedures in the present document;

- SIP MESSAGE requests routed to the terminating participating MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the terminating participating MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element containing a <mcptt-Params> element containing an <emergency-ind> element or an <alert-ind> element. Such requests are known as "SIP MESSAGE requests for emergency notification for terminating participating MCPTT function" in the procedures in the present document;

- SIP MESSAGE requests routed to the controlling MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the controlling MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element containing a <mcptt-Params> element containing an <emergency-ind> element or an <alert-ind> element. Such requests are known as "SIP MESSAGE requests for emergency notification for controlling MCPTT function" in the procedures in the present document;

- SIP MESSAGE requests routed to the originating participating MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the participating MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML

body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <request-type> element set to a value of "private-call-call-back-request" or "private-call-call-back-cancel-request", or with the <response-type> element set to a value of "private-call-call-back-response" or "private-call-call-back-cancel-response". Such requests are known as "SIP MESSAGE request for private call call-back for originating participating MCPTT function";

- SIP MESSAGE requests routed to the terminating participating MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the participating MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <request-type> element set to a value of "private-call-call-back-request" or "private-call-call-back-cancel-request", or with the <response-type> element set to a value of "private-call-call-back-response" or "private-call-call-back-cancel-response".. Such requests are known as "SIP MESSAGE request for private call call-back for terminating participating MCPTT function";

- SIP MESSAGE requests routed to the controlling MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the controlling MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <request-type> element set to a value of "private-call-call-back-request". Such requests are known as "SIP MESSAGE request for private call call-back request for controlling MCPTT function";

- SIP MESSAGE requests routed to the controlling MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the controlling MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <request-type> element set to a value of "private-call-call-back-cancel-request". Such requests are known as "SIP MESSAGE request for private call call-back cancel request for controlling MCPTT function"; and

- SIP MESSAGE requests routed to the controlling MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the controlling MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <response-type> element set to a value of "private-call-call-back-response" or "private-call-call-back-cancel-response". Such requests are known as "SIP MESSAGE request for private call call-back responses for controlling MCPTT function".

- SIP MESSAGE requests routed to the originating participating MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the participating MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <request-type> element set to a value of "group-selection-change-request" or with the <response-type> element set to a value of "group-selection-change-response". Such requests are known as "SIP MESSAGE request for group-selection-change for originating participating MCPTT function";

- SIP MESSAGE requests routed to the terminating participating MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the participating MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <request-type> element set to a value of "group-selection-change-request" or with the <response-type> element set to a value of "group-selection-change -response". Such requests are known as "SIP MESSAGE request for group-selection-change for terminating participating MCPTT function";

- SIP MESSAGE requests routed to the controlling MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the controlling MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <request-type> element set to a value of "group-selection-change-request". Such requests are known as "SIP MESSAGE request for group selection change request for controlling MCPTT function";

- SIP MESSAGE requests routed to the controlling MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the controlling MCPTT function and containing a Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and includes an XML body containing a <mcpttinfo> root element with a <mcptt-Params> element containing an <anyExt> element with the <response-type> element

set to a value of "group-selection-change-response". Such requests are known as "SIP MESSAGE request for group selection change response for controlling MCPTT function".

6.3.1.4 SIP SUBSCRIBE request

The MCPTT server needs to distinguish between the following SIP SUBSCRIBE request for originations and terminations:

- SIP SUBSCRIBE requests routed to the participating MCPTT function with the Request-URI set to the MCPTT session identity identifying the participating MCPTT function and the Event header field set to "conference". Such requests are known as "SIP SUBSCRIBE request for conference event status subscription" in the procedures in the present document;

- SIP SUBSCRIBE requests routed to the controlling MCPTT function with the Request-URI set to the MCPTT session identity identifying the controlling MCPTT function and containing an Event header field set to "conference". Such requests are known as "SIP SUBSCRIBE request for event status subscription in the controlling MCPTT function" in the procedures in the present document; and

- SIP SUBSCRIBE requests routed to the non-controlling MCPTT function with the Request-URI set to the MCPTT session identity identifying the non-controlling MCPTT function and containing an Event header field set to "conference". Such requests are known as "SIP SUBSCRIBE request for event status subscription in the non-controlling MCPTT function" in the procedures in the present document.

6.3.2 Participating MCPTT Function

6.3.2.1 Requests initiated by the served MCPTT user

6.3.2.1.1 SDP offer generation

6.3.2.1.1.1 On-demand session

This subclause is referenced from other subclauses.

The SDP offer is generated based on the received SDP offer. The SDP offer generated by the participating MCPTT function:

1) shall contain only one SDP media-level section for MCPTT speech as contained in the received SDP offer; and

2) shall contain an SDP media-level section for one media-floor control entity, if present in the received SDP offer.

When composing the SDP offer according to 3GPP TS 24.229 [4], the participating MCPTT function:

1) shall replace the IP address and port number for the offered media stream in the received SDP offer with the IP address and port number of the participating MCPTT function, if required;

NOTE 1: Requirements can exist for the participating MCPTT function to be always included in the path of the offered media stream, for example: for the support of features such as MBMS, lawful interception and recording. Other examples can exist.

2) shall replace the IP address and port number for the offered media floor control entity, if any, in the received SDP offer with the IP address and port number of the participating MCPTT function; and

NOTE 2: If the participating MCPTT function and the controlling MCPTT function or the participating MCPTT function and the non-controlling MCPTT function are in the same MCPTT server, and the participating MCPTT function does not have a dedicated IP address or a dedicated port number for media floor control or media stream, the replacement of the IP address or the port number is omitted.

3) shall contain an "a=key-mgmt" attribute field with a "mikey" attribute value, if present in the received SDP offer.

6.3.2.1.1.2 Pre-established session

This subclause is referenced from other subclauses.

When composing an SDP offer according to 3GPP TS 24.229 [4], the participating MCPTT function:

1) shall set the IP address of the participating MCPTT function for MCPTT speech from the SDP negotiated during the pre-established session establishment;

2) shall set the IP address of the participating MCPTT function for the offered media-floor control entity from the SDP negotiated during the pre-established session establishment, if present in the received SDP offer;

3) shall contain only one SDP media-level section for MCPTT speech obtained from the SDP negotiated during the pre-established session establishment consisting of:

   a) the port number for the MCPTT speech; and

   b) the codec(s), media parameters and attributes as in the SDP negotiated during the pre-established session establishment;

4) shall include the media-level section of the offered media-floor control entity from the SDP negotiated during the pre-established session establishment, if any media-floor control entity is offered consisting of:

   a) the media-floor control entity parameters as in the SDP negotiated during the pre-established session establishment; and

   b) the port number for the selected media-floor control entity selected as specified in 3GPP TS 24.229 [4]; and

5) shall contain an "a=key-mgmt" attribute field with a "mikey" attribute value if present in the received SDP offer.

6.3.2.1.2 SDP answer generation

6.3.2.1.2.1 On-demand session

When composing the SDP answer according to 3GPP TS 24.229 [4], the participating MCPTT function:

1) shall replace the IP address and port number in the received SDP answer with the IP address and port number of the participating MCPTT function, for the accepted media stream in the received SDP offer, if required; and

NOTE 1: Requirements can exist for the participating MCPTT function to be always included in the path of the offered media stream, for example: for the support of features such as MBMS, lawful interception and recording. Other examples can exist.

2) shall replace the IP address and port number in the received SDP answer with the IP address and port number of the participating MCPTT function, for the accepted media-floor control entity, if present in the received SDP offer.

NOTE 2: If the participating MCPTT function and the controlling MCPTT function or the participating MCPTT function and the non-controlling MCPTT function are in the same MCPTT server, and the participating MCPTT function does not have a dedicated IP address or a dedicated port number for media floor control or media stream, the replacement of the IP address or the port number is omitted.

6.3.2.1.2.2 Pre-established session establishment

When composing the SDP answer according to 3GPP TS 24.229 [4], the participating MCPTT function:

1. shall set the IP address and port number to those of the participating MCPTT function for each accepted media stream from the list contained in the received SDP offer and for each accepted media stream in the received SDP offer; and

2. shall set the IP address and port number to those of the participating MCPTT function, for the accepted media-floor control entity, if present in the received SDP offer.

6.3.2.1.3 Sending an INVITE request on receipt of an INVITE request

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, 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.

6.3.2.1.4 Sending an INVITE request on receipt of a REFER request

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 REFER request, the participating MCPTT function:

1) shall include in the SIP INVITE request all header fields included in the headers portion of the SIP URI contained in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field in the incoming SIP REFER 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 REFER request to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

5) shall include the g.3gpp.mcptt media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" 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; and

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

8) shall include in the SIP INVITE request an SDP offer as specified in subclause 6.3.2.1.1.2 based upon:

   a) the SDP negotiated during the pre-established session establishment and any subsequent pre-established session modification; and

b) the SDP offer (if any) included in the"body" URI parameter of the SIP-URI contained in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field in the incoming SIP REFER request for a pre-established session;

9) shall determine if the SIP REFER request is regarded as being received with an implicit floor request;

a) if according to subclause 6.4, the SIP REFER request is regarded as being received with an implicit floor request, the participating MCPTT function shall include the "mc_implicit_request" media level attribute in the associated UDP stream for the floor control in the SDP offer of the SIP INVITE request; and

b) if, according to subclause 6.4, the SIP REFER request is regarded as being not received with an implicit floor request, the participating MCPTT function shall not include the "mc_implicit_request" media level attribute in the associated UDP stream for the floor control in the SDP offer of the SIP INVITE request;

10) shall determine if the SIP REFER request is regarded as being received with an implicit request to grant the floor to the terminating MCPTT client;

a) if according to subclause 6.4, the SIP REFER request is regarded as being received with an implicit request to grant the floor to the terminating MCPTT client, the participating MCPTT function shall include the "mc_implicit_request" media level attribute in the associated UDP stream for the floor control in the SDP offer of the SIP INVITE request; and

b) if, according to subclause 6.4, the SIP REFER request is regarded as being not received with an implicit request to grant the floor to the terminating MCPTT client, the participating MCPTT function shall not include the "mc_implicit_request" media level attribute in the associated UDP stream for the floor control in the SDP offer of the SIP INVITE request;

11) shall copy the application/vnd.3gpp.mcptt-info+xml MIME body from the "body" URI header field of the SIP-URI in the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field of the SIP REFER request, to the outgoing SIP INVITE request;

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

13) if the incoming SIP REFER request contained an application/resource-lists MIME body in the "body" URI header field of the SIP-URI contained in the <entry> element of an application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field, shall copy the application/resources-lists MIME body in the "body" URI header field to the SIP INVITE request;

6.3.2.1.5 Response to an INVITE request

6.3.2.1.5.1 Provisional responses

NOTE: This subclause is referenced from other procedures

When sending SIP provisional responses other than the SIP 100 (Trying) response, the participating MCPTT function shall generate a SIP provisional response according to 3GPP TS 24.229 [4] and:

1) 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";

c) the isfocus media feature tag; and

d) an MCPTT session identity mapped to the MCPTT session identity if provided in the Contact header field of the incoming provisional response;

2) shall include the "norefersub" option tag in a Supported header field in accordance with 3GPP TS 24.229 [4];

3) may include a Resource-Share header field in accordance with subclause 5.7.1.20.2 in 3GPP TS 24.229 [4]; and

4) if the incoming SIP provisional 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 provisional response.

6.3.2.1.5.2 Final response

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.

6.3.2.1.6 Sending a SIP BYE request on receipt of a SIP BYE request

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;

5) if the received SIP BYE request contains an application/vnd.3gpp.mcptt-info+xml MIME body, shall copy the application/vnd.3gpp.mcptt-info+xml MIME body into the outgoing SIP BYE request; and

6) 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.

6.3.2.1.7 Sending a SIP BYE request on receipt of a SIP REFER request

Upon receiving a SIP REFER request with the "method" SIP URI parameter set to value "BYE" in the URI in the Refer-To header field from the MCPTT client, the participating MCPTT function:

1) if the user identified by the MCPTT ID is not authorised, shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response to the SIP BYE request, with warning text set to "100 function not allowed due to <detailed reason>" as specified in subclause 4.4, and shall not continue with the rest of the steps;

2) if the SIP REFER request contained a Refer-Sub header field containing "false" value and a Supported header field containing "norefersub" value, shall handle the SIP REFER request as specified in 3GPP TS 24.229 [4],

IETF RFC 3515 [25] as updated by IETF RFC 6665 [26], and IETF RFC 4488 [22] without establishing an implicit subscription;

3) shall generate a SIP 200 (OK) response to the SIP REFER request, and in the SIP 200 (OK) response:

   a) shall include the Supported header field with value "norefersub" according to rules and procedures of IETF RFC 4488 [22]; and

   b) shall check the presence of the Refer-Sub header field of the SIP REFER request and if it is present and set to the value "false" shall include the Refer-Sub header field with value "false" according to rules and procedures of IETF RFC 4488 [22];

NOTE: In accordance with IETF RFC 4488 [22], the participating MCPTT function inserts the Refer-Sub header field containing the value "false" in the SIP 200 (OK) response to the SIP REFER request to indicate that it has not created an implicit subscription.

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

5) shall generate a SIP BYE request, and in the SIP BYE request:

   a) shall set the Request-URI to the MCPTT session identity which was included at the Refer-To header field of the received REFER request; and

   b) shall copy the contents of the P-Asserted-Identity header field of the received REFER request to the P-Asserted-Identity header field of the outgoing SIP BYE request; and

6) 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 participating MCPTT function 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.

6.3.2.1.8 Priority call conditions

6.3.2.1.8.0 General

The subclauses of the parent subclause contain common procedures to be used for MCPTT emergency group calls and MCPTT imminent peril group calls.

6.3.2.1.8.1 Determining authorisation for originating a priority group call

When the participating MCPTT function receives a request from the MCPTT client to originate an MCPTT emergency group call and needs to determine if the request is an authorised request for an MCPTT emergency call, the participating MCPTT function shall check the following:

1) if the <allow-emergency-group-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true" and:

   a) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> element contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "DedicatedGroup" and if the <uri-entry> element of the <entry> element of the <MCPTTGroupInitiation> element contains the identity of the MCPTT group targeted by the calling MCPTT user; or

   b) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UseCurrentlySelectedGroup";

   then the participating MCPTT function shall consider the MCPTT emergency group call request to be an authorised request for an MCPTT emergency group call;

In all other cases, the participating MCPTT function shall consider the request to originate an MCPTT emergency group call to be an unauthorised request to originate an MCPTT emergency group call.

When the participating MCPTT function receives a request from the MCPTT client to originate an MCPTT imminent peril group call and needs to determine if the request is an authorised request for an MCPTT imminent peril group call the participating MCPTT function shall check the following:

1) if the <allow-imminent-peril-call> element of <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true"; and

   a) if the "entry-info" attribute of the <MCPTTGroupInitiation> element contained within the <ImminentPerilCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "DedicatedGroup" and if the <uri-entry> element of the <entry> element of the <MCPTTGroupInitiation> element contains the identity of the MCPTT group targeted by the calling MCPTT user; or

   b) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element contained within the <ImminentPerilCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UseCurrentlySelectedGroup";

   then the participating MCPTT function shall consider the MCPTT imminent peril group call request to be an authorised request for an MCPTT emergency group call;

In all other cases, the participating MCPTT function shall consider the request to originate an MCPTT imminent peril group call to be an unauthorised request to originate an MCPTT imminent peril call.

6.3.2.1.8.2 Determining authorisation for initiating or cancelling an MCPTT emergency alert

If the participating MCPTT function receives a SIP request from the MCPTT client including a request for an MCPTT emergency alert and:

1) if the <allow-activate-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling MCPTT user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true"; and

2) if the "entry-info" attribute of the <entry> element of the <EmergencyAlert> element contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of:

   a) "DedicatedGroup", and if the <uri-entry> element of the <entry> element of the <EmergencyAlert> element of the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) contains the MCPTT group identity of the MCPTT group targeted by the calling MCPTT user; or

   b) "UseCurrentlySelectedGroup" and the <allow-MCPTT-emergency-alert> element of the <list-element> of the group document identified by the MCPTT group identity targeted for the emergency alert is set to a value of "true" as specified in 3GPP TS 24.481 [31].

then the MCPTT emergency alert request shall be considered to be an authorised request for an MCPTT emergency alert. In all other cases, it shall be considered to be an unauthorised request for an MCPTT emergency alert.

If the participating MCPTT function receives a SIP request from the MCPTT client including a request to cancel an MCPTT emergency alert to an MCPTT group, and if the <allow-cancel-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling MCPTT user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true", then the MCPTT emergency alert cancellation request shall be considered to be an authorised request to cancel an MCPTT emergency alert. In all other cases, it shall be considered to be an unauthorised request to cancel an MCPTT emergency alert.

6.3.2.1.8.3 Validate priority request parameters

This subclause is referenced from other procedures.

To validate the combinations of <emergency-ind>, <imminentperil-ind> and <alert-ind> which are received in SIP requests, the participating MCPTT function shall follow the procedures specified in subclause 6.3.3.1.17.

6.3.2.1.8.4 Retrieving Resource-Priority header field values

This subclause is referenced from other procedures.

The participating MCPTT function shall follow the procedures specified in subclause 6.3.3.1.19 with the clarification that references in that procedure to the controlling MCPTT function should be replaced with references to the participating MCPTT function.

6.3.2.1.8.5 Generating a SIP re-INVITE request for priority group call origination within a pre-established session

This subclause is referenced from other procedures.

Upon receipt of a SIP 2xx response which does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149" to a SIP INVITE request sent to the controlling MCPTT function which contained a Resource-Priority header field populated for an MCPTT emergency group call or MCPTT imminent peril group call as specified in subclause 6.3.2.1.8.4, the participating MCPTT function:

1) shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] to be sent within the SIP dialog of the pre-established session;

2) shall include in the SIP re-INVITE request an SDP offer based upon the previously negotiated SDP for the pre-established session;

3) shall include in the SIP re-INVITE request a Resource-Priority header field with the contents set as in the Resource-Priority header field included in the SIP INVITE request sent to the controlling MCPTT function; and

4) shall skip the remaining steps.

NOTE 1: This is the case where the MCPTT client's previously sent SIP REFER request was either 1) a request for an MCPTT emergency group call or MCPTT imminent peril group call or 2), was not a request for an MCPTT emergency group call or MCPTT imminent peril group call but targeted an MCPTT group which is in an in-progress emergency group state or in-progress imminent peril group state. In either case no SIP INFO pending warning was expected or received.

Upon receipt of a SIP 2xx response from the controlling MCPTT function to a request for an MCPTT emergency call or MCPTT imminent peril call, that contains a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", the participating MCPTT function shall wait for the receipt of a SIP INFO request from the controlling MCPTT function.

Upon receipt of a SIP INFO request from the controlling MCPTT function within the dialog of the SIP INVITE request for an MCPTT emergency call or MCPTT imminent peril call, the participating MCPTT function:

1) shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] to be sent within the SIP dialog of the pre-established session;

2) shall include in the SIP re-INVITE request an SDP offer based upon the previously negotiated SDP for the pre-established session;

3) shall include in the SIP re-INVITE request a Resource-Priority header field with the contents set as in the Resource-Priority header field included in shall include a Resource-Priority header field with the contents set as in the SIP INVITE request sent to the controlling MCPTT function; and

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

   a) an <emergency-ind> element if included in the application/vnd.3gpp.mcptt-info+xml MIME body contained in the received SIP INFO request, set to the value of the <emergency-ind> in the SIP INFO request;

   b) an <alert-ind> element if included in the application/vnd.3gpp.mcptt-info+xml MIME body contained in the received SIP INFO request, set to the value of the <alert-ind> in the SIP INFO request; and

c) an <imminentperil-ind> element if included in the application/vnd.3gpp.mcptt-info+xml MIME body contained in the received SIP INFO request, set to the value of the <imminentperil-ind> in the SIP INFO request.

NOTE 2: This is the case where the MCPTT client's previously sent SIP REFER request was a request for an MCPTT emergency group call or an MCPTT imminent peril group call and a SIP INFO request was received in the dialog with the controlling MCPTT function for the MCPTT emergency group call or MCPTT imminent peril group call.

6.3.2.1.8.6 Generating a SIP re-INVITE request for emergency private call origination within a pre-established session

This subclause is referenced from other procedures.

Upon receipt of a SIP 2xx response which does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149" to a SIP-INVITE request sent to the controlling MCPTT function which contained a Resource-Priority header field populated for an MCPTT emergency private call as specified in subclause 6.3.2.1.8.4, the participating MCPTT function:

1) shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] to be sent within the SIP dialog of the pre-established session;

2) shall include in the SIP re-INVITE request an SDP offer:

   a) based upon the previously negotiated SDP for the pre-established session; and

   b) if the received SIP 2xx response was in response to a request for a first-to-answer call and the SDP answer contained an a=key-mgmt attribute, shall include the a=key-mgmt attribute and its value in the SDP offer as specified in IETF RFC 4567 [47];

3) shall include in the SIP re-INVITE request a Resource-Priority header field with the contents set as in the Resource-Priority header field included in the SIP INVITE request sent to the controlling MCPTT function; and

4) shall skip the remaining steps.

NOTE 1: This is the case where the MCPTT client's previously sent SIP REFER request was either 1) a request for an MCPTT emergency private call or 2), was not a request for an MCPTT emergency private call but MCPTT emergency private priority state was already set to "in-progress". In either case no SIP INFO pending warning was expected or received.

Upon receipt of a SIP 2xx response from the controlling MCPTT function to a request for an MCPTT emergency private call, that contains a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", the participating MCPTT function shall wait for the receipt of a SIP INFO request from the controlling MCPTT function.

Upon receipt of a SIP INFO request from the controlling MCPTT function within the dialog of the SIP INVITE request for an MCPTT emergency private call, the participating MCPTT function :

1) shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] to be sent within the SIP dialog of the pre-established session;

2) shall include in the SIP re-INVITE request an SDP offer:

   a) based upon the previously negotiated SDP for the pre-established session; and

   b) if the received SIP 2xx response was in response to a request for a first-to-answer call and the SDP answer contained an a=key-mgmt attribute, shall include the a=key-mgmt attribute and its value in the SDP offer as specified in IETF RFC 4567 [47];

3) shall include in the SIP re-INVITE request a Resource-Priority header field with the contents set as in the Resource-Priority header field included in the SIP INVITE request sent to the controlling MCPTT function; and

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

a) an <alert-ind> element if included in the application/vnd.3gpp.mcptt-info+xml MIME body contained in the received SIP INFO request, set to the value of the <alert-ind> in the SIP INFO request.

NOTE 2: This is the case where the MCPTT client's previously sent SIP REFER request was a request for an MCPTT emergency private call and a SIP INFO request was received in the dialog with the controlling MCPTT function for the MCPTT emergency private call.

6.3.2.1.8.7 Generating a SIP re-INVITE request for first-to-answer call origination within a pre-established session

This subclause is referenced from other procedures.

Upon receipt of a SIP 2xx response to a SIP INVITE request for a first-to-answer call which contains an SDP answer including an a=key-mgmt attribute, the participating MCPTT function:

1) shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] to be sent within the SIP dialog of the pre-established session; and

2) shall include in the SIP re-INVITE request an SDP offer:

   a) based upon the previously negotiated SDP for the pre-established session; and

   b) containing the a=key-mgmt attribute and value as received in the SDP answer in the SDP offer as specified in IETF RFC 4567 [47].

6.3.2.1.9 Generating a SIP re-INVITE request on receipt of a SIP re-INVITE request

This subclause is referenced from other procedures.

When generating a SIP re-INVITE request according to 3GPP TS 24.229 [4] on receipt of an incoming SIP re-INVITE request, the participating MCPTT function:

1) if the incoming SIP re-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];

2) if the incoming SIP re-INVITE request contained an application/vnd.3gpp.mcptt-info+xml MIME body, shall copy the application/vnd.3gpp.mcptt-info+xml MIME body; and

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

6.3.2.1.10 Sending a SIP INVITE request on receipt of SIP 3xx response

This subclause is referenced from other procedures.

Upon:

1) receipt of a SIP INVITE request or SIP REFER request from the MCPTT client;

2) having sent a SIP INVITE request to the controlling MCPTT function; and

3) having received a SIP 302 (Moved Temporarily) response from the controlling MCPTT function with:

   a) a Contact header field containing a SIP-URI; and

   b) an application/vnd.3gpp.mcptt-info+xml MIME body with an <mcptt-request-uri> element;

the participating MCPTT function:

1) shall generate a SIP INVITE request with the Request-URI set to the contents of the Contact header field of the SIP 302 (Moved Temporarily) response;

2) 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 original incoming SIP INVITE or SIP REFER request from the MCPTT client;

3) 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";

4) shall include the option tag "timer" in the Supported header field;

5) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP INVITE or SIP REFER request from the client to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

6) shall include the g.3gpp.mcptt media feature tag into the Contact header field of the outgoing SIP INVITE request;

7) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the outgoing SIP INVITE request;

8) 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;

9) if an SIP INVITE request was received from the client containing 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 original incoming SIP INVITE request to the outgoing SIP INVITE request;

10) if a SIP REFER request was received from the client with a "cid" URL pointing to an application/resource-lists MIME body as specified in IETF RFC 5366 [20] containing SIP-URI with a "body" URI header field containing an application/vnd.3gpp.mcptt-info MIME body, shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body un the INVITE request to the outgoing SIP INVITE request;

11) shall copy the contents of the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body received in the SIP 302 (Moved Temporarily) response, to the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the outgoing SIP INVITE request;

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 that was determined when the participating MCPTT function received the SIP INVITE request or SIP REFER request from the client ; and

13) if the <session-type> element is received in the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP 3xx response, shall set the <session-type> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request to the value of the <session-type> element received in the SIP 3xx response.

6.3.2.2 Requests terminated to the served MCPTT user

6.3.2.2.1 SDP offer generation

The participating MCPTT function shall follow the procedures in subclause 6.3.2.1.1.

6.3.2.2.2 SDP answer generation

6.3.2.2.2.1 On-demand session

The participating MCPTT function shall follow the procedures in subclause 6.3.2.1.2.1.

6.3.2.2.2.2 Pre-established session

When composing an SDP answer according to 3GPP TS 24.229 [4], the MCPTT server:

1) shall set the IP address of the MCPTT server for the accepted MCPTT speech media stream from the received SDP offer, which was also negotiated during the pre-established session establishment;

2) shall set the IP address of the MCPTT server for the accepted media-floor control entity from the received SDP offer, which was also negotiated during the pre-established session establishment, if present in the received SDP offer;

3) shall include the media-level section for the accepted MCPTT speech media stream from the received SDP offer, which was also negotiated in pre-established session establishment, consisting of:

   a) the port number for MCPTT speech; and

   b) the codec(s) and media parameters selected by the MCPTT server from the received SDP offer; and

4) shall include for the media-floor control entity, that is offered in the SDP offer from the MCPTT server and accepted in the SDP answer by MCPTT client, the media-level section of each offered media-floor control entity consisting of:

   a) the media-floor control entity parameters contained in the received SDP offer, restricted to media-floor control entity parameters negotiated during the pre-established session establishment; and

   b) the port number for selected media-floor control entity selected as specified in 3GPP TS 24.229 [4].

6.3.2.2.3 SIP INVITE request towards the terminating MCPTT client

The participating MCPTT function shall generate an initial SIP INVITE request according to 3GPP TS 24.229 [4] and:

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 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";

   c) the isfocus media feature tag;

   d) an MCPTT session identity mapped to the MCPTT session identity provided in the Contact header field of the incoming SIP INVITE request; and

   e) any other uri-parameter provided in the Contact header field of the incoming SIP INVITE request;

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

6) shall include the option tag "norefersub" in a Supported header field according to rules and procedures of IETF RFC 4488 [22];

7) may include a Resource-Share header field in accordance with subclause 5.7.1.20.3 in 3GPP TS 24.229 [4]; and

8) 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 SIP INVITE request.

6.3.2.2.4 Response to a SIP INVITE request

6.3.2.2.4.1 Provisional response

This subclause is referenced from other procedures.

When sending a SIP provisional response other than the SIP 100 (Trying) response to the SIP INVITE request, the participating MCPTT function shall generate a SIP provisional response according to 3GPP TS 24.229 [4] and:

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

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

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

2) if the outgoing SIP provisional response is to be sent in response to the receipt of a SIP provisional response and the response contains an application/vnd.3gpp.mcptt-info+xml MIME body, shall copy the application/vnd.3gpp.mcptt-info+xml MIME body to the outgoing SIP provisional response; and

3) if the incoming SIP INVITE request included the Supported header field with the value "100rel" and according to local policy, may include the Require header field with the value "100rel".

6.3.2.2.4.2 Final response

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.

6.3.2.2.5 Automatic Commencement Mode

6.3.2.2.5.1 General

When receiving a "SIP INVITE request for terminating participating MCPTT function" that requires automatic commencement mode:

1) if:

   a) the invited MCPTT client has one or more pre-established sessions without an associated MCPTT session;

   b) the media-level section for the offered MCPTT speech media stream is the same as the media-level section for MCPTT speech media stream in an existing pre-established session; and

   c) the media-level section of the offered media-floor control entity is the same as the media-level section for media-floor control entity in an existing pre-established session;

   then the participating MCPTT function shall perform the actions specified in subclause 6.3.2.2.5.3; or

2) otherwise the participating MCPTT function shall perform the actions specified in subclause 6.3.2.2.5.2.

6.3.2.2.5.2 Automatic commencement for On-Demand session

When receiving a "SIP INVITE request for terminating participating MCPTT function" for an on-demand session that requires automatic commencement mode the participating MCPTT function:

1) if:

   a) the incoming SIP INVITE request contained a Priv-Answer-Mode header field set to the value of "Auto";

   b) no Answer-Mode header field or Priv-Answer-Mode header field were received in the incoming SIP INVITE request and the Answer-Mode Indication received in the application/poc-settings+xml MIME body received from the invited MCPTT client as defined in subclause 7.3.3 or subclause 7.3.4 is set to "auto-answer"; or

   c) the incoming SIP INVITE request contained an Answer-Mode header field set to "Auto" and the Answer-Mode Indication received in the application/poc-settings+xml MIME body received from the invited MCPTT client as defined in subclause 7.3.3 or subclause 7.3.4 is set to "auto-answer";

   then:

   a) shall generate a SIP 183 (Session Progress) response to the "SIP INVITE request for terminating participating MCPTT function" as specified in subclause 6.3.2.2.4.1;

   b) if the received SIP INVITE request contained an application/vnd.3gpp.mcptt-info+xml MIME body with the <ambient-listening-type> element set to a value of "remote-init" shall include in the SIP 183 (Session Progress) response an alert-info header field set to a value of "<file:///dev/null>" according to IETF RFC 3261 [24] and as updated by IETF RFC 7462 [77]; and

NOTE: The SIP 183 (session Progress) response can be sent reliably or unreliably depending on the content of the received SIP INVITE request. Regardless of if the SIP 183 (Session Progress) response is sent reliably or unreliably, SDP is not included in the SIP 183 (Session Progress) response.

   c) shall set the P-Answer-State header field to "Unconfirmed" in the SIP 183 (Session Progress) response;

2) shall copy the public user identity contained in the Request-URI of the incoming "SIP INVITE request for terminating participating MCPTT function" to the P-Asserted-Identity header field of the SIP 183 (Session Progress) response;

3) shall generate a SIP INVITE request as specified in subclause 6.3.2.2.3;

4) shall set the Request-URI to the public user identity associated to the MCPTT ID of the MCPTT user to be invited;

5) shall perform the procedures specified in subclause 6.3.2.2.9 to include any MIME bodies in the received SIP INVITE request, into the outgoing SIP INVITE request;

6) shall copy the contents of the P-Asserted-Identity header field of the incoming "SIP INVITE request for terminating participating MCPTT function" to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

7) if the Priv-Answer-Mode header field is present in the incoming SIP INVITE request with a value of "Auto", shall include a Priv-Answer-Mode header field with the value "Auto" in the outgoing SIP INVITE request. Otherwise, if the Answer-Mode header field is present in the incoming SIP INVITE request, the participating MCPTT function shall include an Answer-Mode header field with the value "Auto" in the outgoing SIP INVITE request;

8) if no Answer-Mode header field or Priv-Answer-Mode header field were received in the incoming SIP INVITE request and the Answer-Mode Indication received in the application/poc-settings+xml MIME body received from the invited MCPTT client as defined in subclause 7.3.3 or subclause 7.3.4 is set to "auto-answer", shall set the Answer-Mode header field to "Auto" in the outgoing SIP INVITE request;

9) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received "SIP INVITE request for terminating participating MCPTT function" as specified in subclause 6.3.2.2.1;

10) if the received SIP INVITE request contains a Resource-Priority header field, shall include a Resource-Priority header field with the contents set as in the received Resource-Priority header field; and

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

If the SIP 183 (Session Progress) response was sent reliably, then upon receiving a SIP PRACK request, the participating MCPTT function shall generate a SIP 200 (OK) response to the SIP PRACK request and forward the SIP 200 (OK) response, according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the above SIP INVITE request sent to the MCPTT client, the participating MCPTT function:

1) if the SIP 183 (Session Progress) was sent unreliably, shall send the SIP 200 (OK) response immediately; and

2) if the SIP 183 (Session Progress) was sent reliably and,

   a) if the SIP PRACK request to the SIP 183 (Session Progress) response has been received by the participating MCPTT function and the SIP 200 (OK) response to the SIP PRACK request has been sent, shall send the SIP 200 (OK) response immediately;

   b) if the SIP PRACK request to the SIP 183 (Session Progress) response has not yet been received, then upon receipt of the SIP PRACK request, the participating MCPTT function shall generate a SIP 200 (OK) response to the SIP PRACK request and forward the SIP 200 (OK) response, according to 3GPP TS 24.229 [4], before sending the SIP 200 (OK) response to the "SIP INVITE request for terminating participating MCPTT function".

When the participating MCPTT function sends the SIP 200 (OK) response to the "SIP INVITE request for terminating participating MCPTT function", the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as described in the subclause 6.3.2.2.4.2;

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 6.3.2.2.2.1;

3) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

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

5) shall forward the SIP 200 (OK) response according to 3GPP TS 24.229 [4].

The participating MCPTT function shall forward any other SIP response that does not contain SDP along the signalling path to the originating network according to 3GPP TS 24.229 [4].

6.3.2.2.5.3 Automatic commencement for pre-established session

NOTE: This subclause is referenced from other procedures.

When receiving a "SIP INVITE request for terminating participating MCPTT function" for a pre-established session that requires automatic commencement mode the participating MCPTT function:

1) if the received SIP INVITE request contains:

   a) an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "true"; or

   b) a Priv-Answer-Mode header field;

      i) shall perform the procedures of subclause 6.3.2.2.5.2 with the following clarifications:

         A) include in the outgoing SIP INVITE request a Replaces header field populated with the call-id, to-tag and from-tag of the targeted pre-established session as specified in IETF RFC 3891 [65];

         B) include in the SDP offer the current media parameters used by the targeted pre-established session identified by the Replaces header field;

         C) if the SIP core supports resource sharing, include in the outgoing SIP INVITE request a Resource-Share header field as specified in 3GPP TS 24.229 [4] with:

i) the value "media-sharing";

ii) an "origin" header field parameter set to "session-receiver";

iii) a "timestamp" header field parameter; and

iv) a "rules" header field parameter with one resource sharing rule per media stream in the same order the corresponding m-line appears in the SDP. Each resource sharing rule is constructed as follows:

- a "new-sharing-key" part containing the same key as that included when the media bearer for the pre-established session was established; and

- a "directionality" part indicating the direction of the pre-established media bearer; and

c) shall skip the remaining steps;

2) shall generate a SIP 200 (OK) response to the "SIP INVITE request for terminating participating MCPTT function" as described in the subclause 6.3.2.2.4.2;

3) shall include in the SIP 200 (OK) response an SDP answer as specified in the subclause 6.3.2.2.2.2 based on the SDP negotiated during the pre-established session establishment and SDP offer received in the "SIP INVITE request for terminating participating MCPTT function";

4) shall set the P-Answer-State header field to "Unconfirmed" in the SIP 200 (OK) response;

5) shall set the P-Asserted-Identity header field to the same value as included in the SIP INVITE request that was sent by the MCPTT client when the pre-established session was established, in the SIP 200 (OK) response;

6) shall send the SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [4]; and

7) shall interact with the media plane as specified in 3GPP TS 24.380 [5] clause 9.

6.3.2.2.6 Manual Commencement Mode

6.3.2.2.6.1 General

When receiving a "SIP INVITE request for terminating participating MCPTT function" that requires manual commencement mode:

1) if:

a) the invited MCPTT client has one or more pre-established sessions without an associated MCPTT session;

b) the media-level section for the offered MCPTT speech media stream is the same as the media-level section for MCPTT speech media stream in the existing pre-established session; and

c) the media-level section of the offered media-floor control entity is the same as the media-level section for media-floor control entity in the existing pre-established session;

then the participating MCPTT function shall perform the actions specified in subclause 6.3.2.2.6.3; or

2) otherwise the participating MCPTT function shall perform the actions specified in subclause 6.3.2.2.6.2.

6.3.2.2.6.2 Manual commencement for On-Demand session

When receiving a "SIP INVITE request for terminating participating MCPTT function" for an on-demand session that requires manual commencement mode the participating MCPTT function:

1) shall generate a SIP INVITE request as specified in subclause 6.3.2.2.3;

2) shall set the Request-URI to the public user identity associated to the MCPTT ID of the MCPTT user to be invited;

3) shall perform the procedures specified in subclause 6.3.2.2.9 to include any MIME bodies in the received SIP INVITE request;

4) if the Answer-Mode header field is present in the incoming SIP INVITE request, participating MCPTT function, shall include an Answer-Mode header field with the value "Manual";

5) if no Answer-Mode header field was received in the incoming SIP INVITE request and the Answer-Mode Indication received in the application/poc-settings+xml MIME body received from the invited MCPTT client as defined in subclause 7.3.3 or subclause 7.3.4 is set to "manual-answer", shall set the Answer-Mode header field to "Manual" in the outgoing SIP INVITE request;

6) if the Priv-Answer-Mode header field is present in the incoming SIP INVITE request, the participating MCPTT function shall include a Priv-Answer-Mode header field with the value "Manual";

7) shall copy the contents of the P-Asserted-Identity header field of the incoming "SIP INVITE request for terminating participating MCPTT function" to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

8) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received "SIP INVITE request for terminating participating MCPTT function" as specified in subclause 6.3.2.2.1;

9) if the received SIP INVITE request contains a Resource-Priority header field, shall include a Resource-Priority header field with the contents set as in the received Resource-Priority header field; and

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

Upon receiving a SIP 180 (Ringing) response to the above SIP INVITE request, the participating MCPTT function:

NOTE 1: A SIP 180 (Ringing) response is received from a terminating MCPTT client in the case of a private call or first-to-answer call.

1) shall generate a SIP 180 (Ringing) response as specified in subclause 6.3.2.2.4.1;

2) shall include the P-Asserted-Identity header field as received in the incoming SIP 180 (Ringing) response; and

3) shall forward the SIP 180 (Ringing) response according to 3GPP TS 24.229 [4].

Upon receiving a SIP 183 (Session Progress) response to the above SIP INVITE request, the participating MCPTT function:

NOTE 2: A SIP 183 (Session Progress) response can be received from a terminating MCPTT client in the case of a group call.

1) shall generate a SIP 183 (Session Progress) response as specified in subclause 6.3.2.2.4.1;

2) shall include the P-Asserted-Identity header field as received in the incoming SIP 183 (Session Progress) response;

3) shall include the P-Answer-State header field if received in the incoming SIP 183 (Session Progress) request; and

4) shall forward the SIP 183 (Session Progress) response according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the SIP INVITE request sent to the MCPTT client, the participating MCPTT function:

When the participating MCPTT function sends the SIP 200 (OK) response the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as described in the subclause 6.3.2.2.4.2;

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 6.3.2.2.2.1;

3) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

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

5) shall forward the SIP 200 (OK) response according to 3GPP TS 24.229 [4].

The participating MCPTT function shall forward any other SIP response that does not contain SDP along the signalling path to the originating network according to 3GPP TS 24.229 [4].

6.3.2.2.6.3 Manual commencement for Pre-established session

When receiving a "SIP INVITE request for terminating participating MCPTT function" for a pre-established session that requires manual commencement mode the participating MCPTT function:

Editor's Note: The functionality in step 1) needs to be made generic, by moving it to clause 8. This is TBD.

1) if:

   a) the received SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "true"; or

   b) if the Priv-Answer-Mode header field is present in the incoming SIP INVITE request;

   then:

   a) shall perform the procedures of subclause 6.3.2.2.6.2 with the following clarifications:

      i) include in the outgoing SIP INVITE request a SIP Replaces header field populated with the call-id, to-tag and from-tag of the targeted pre-established session as specified in IETF RFC 3891 [65];

      ii) include in the SDP offer the current media parameters used by the targeted pre-established session identified by the Replaces header field; and

      iii) if the SIP core supports resource sharing, include in the outgoing SIP INVITE request a Resource-Share header field as specified in 3GPP TS 24.229 [4] with:

         A) the value "media-sharing";

         B) an "origin" header field parameter set to "session-receiver";

         C) a "timestamp" header field parameter; and

         D) a "rules" header field parameter with one resource sharing rule per media stream in the same order the corresponding m-line appears in the SDP. Each resource sharing rule is constructed as follows:

            - a "new-sharing-key" part containing the same key as that included when the media bearer for the pre-established session was established; and

            - a "directionality" part indicating the direction of the pre-established media bearer; and

   b) shall skip the remaining steps;

2) shall generate a SIP re-INVITE request as described in subclause 6.3.2.2.3;

NOTE 1: A SIP re-INVITE request cannot include an Answer-Mode header field as specified in IETF RFC 5373 [18] so Manual Answer is implied with a SIP re-INVITE request within the existing SIP dialog of the pre-established session.

3) shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming "SIP INVITE request for terminating participating MCPTT function" to the outgoing SIP re-INVITE request;

4) shall include in the SIP re-INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request as specified in the subclause 6.3.2.2.1; and

5) shall send the SIP re-INVITE request towards the MCPTT client according to 3GPP TS 24.229 [4];

Upon receiving a SIP 180 (Ringing) response to the above SIP re-INVITE request, the participating MCPTT function:

NOTE 2: A SIP 180 (Ringing) response is received from a terminating MCPTT client in the case of a private call.

1) shall generate a SIP 180 (Ringing) response as specified in subclause 6.3.2.2.4.1;

2) shall include the P-Asserted-Identity header field as received in the incoming SIP 180 (Ringing) response; and

3) shall forward the SIP 180 (Ringing) response according to 3GPP TS 24.229 [4].

Upon receiving a SIP 183 (Session Progress) response to the above SIP re-INVITE request, the participating MCPTT function:

NOTE 3: A SIP 183 (Session Progress) response can be received from a terminating MCPTT client in the case of a group call.

1) shall generate a SIP 183 (Session Progress) response as specified in subclause 6.3.2.2.4.1;

2) shall include the P-Asserted-Identity header field as received in the incoming SIP 183 (Session Progress) response;

3) shall include the P-Answer-State header field as received in the incoming SIP 183 (Session Progress) request; and

4) shall forward the SIP 183 (Session Progress) response according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request, the participating MCPTT function:

1) if the received SDP answer includes changes in codecs or media formats, shall interact with the media plane as specified in 3GPP TS 24.380 [5] for updating the media plane with the newly negotiated codecs and media parameters from the received SDP answer;

2) shall generate a SIP 200 (OK) response as described in the subclause 6.3.2.2.4.2;

3) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

4) shall include in the SIP 200 (OK) response, an SDP answer based on the SDP answer in the received SIP 200 (OK) response, as specified in subclause 6.3.2.2.2.1;

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

NOTE 4: The participating MCPTT function sends a MCCP Connect message, in order to give MCPTT session identity to the terminating MCPTT client.

6) shall send the SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [4].

6.3.2.2.7 Void

6.3.2.2.8 SIP BYE request towards the terminating MCPTT client

6.3.2.2.8.1 On-demand

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;

4) if the received SIP BYE request contains an application/vnd.3gpp.mcptt-info+xml MIME body, shall copy the application/vnd.3gpp.mcptt-info+xml MIME body into the outgoing SIP BYE request; and

5) 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.

6.3.2.2.8.2 Using pre-established session

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 9.3 in 3GPP TS 24.380 [5] for disconnecting the media plane resources towards the controlling MCPTT function;

2) shall send a SIP 200 (OK) response to the controlling MCPTT function;

3) shall interact with the media plane as specified in 3GPP TS 24.380 [5] for disconnecting media plane resources towards the MCPTT client from the media plane resources towards the controlling MCPTT function; and

4) shall maintain the pre-established session towards the MCPTT client.

6.3.2.2.9 Populate MIME bodies

This subclause is referenced from other procedures.

If the incoming SIP request contains an application/vnd.3gpp.mcptt-info+xml MIME body, the participating MCPTT function:

1) if not already copied:

   a) shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body received in the SIP request into an application/vnd.3gpp.mcptt-info+xml MIME body included in the outgoing SIP request; and

   b) if an <MKFC-GKTP> element was included in the application/vnd.3gpp.mcptt-info+xml MIME body received in the SIP request, the <MKFC-GKTP> element shall not be copied into the application/vnd.3gpp.mcptt-info+xml MIME body included in the outgoing SIP request.

If the received SIP request contains an application/vnd.3gpp.location-info+xml MIME body as specified in Annex F.3:

1) if not already copied, shall copy the contents of the application/vnd.3gpp.mcptt-location-info+xml MIME body received in the SIP request into an application/vnd.3gpp.mcptt-location-info+xml MIME body included in the outgoing SIP request.

If the received SIP request contains an application/resource-lists+xml MIME body:

1) if not already copied, shall copy the contents of the application/resource-lists+xml MIME body received in the SIP request into an application/resource-lists+xml MIME body included in the outgoing SIP request.

6.3.2.2.10 Generating a SIP re-INVITE request towards the terminating MCPTT client

This subclause is referenced from other procedures.

The participating MCPTT function shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4] and:

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

2) may include a Resource-Share header field in accordance with subclause 5.7.1.20.3 in 3GPP TS 24.229 [4];

3) shall perform the procedures specified in subclause 6.3.2.2.9 to copy any MIME bodies in the received SIP re-INVITE request to the outgoing SIP re-INVITE request; and

4) if the received SIP re-INVITE request contains a Resource-Priority header field, shall include a Resource-Priority header field with the contents set as in the received Resource-Priority header field.

6.3.2.2.11 Generating a SIP MESSAGE request towards the terminating MCPTT client

This subclause is referenced from other procedures.

The participating MCPTT function shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] and:

1) shall include in the SIP MESSAGE 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] that were received (if any) in the incoming SIP MESSAGE request;

2) shall set the Request-URI of the outgoing SIP MESSAGE request to the public user identity associated to the MCPTT ID of the terminating MCPTT user;

3) shall populate the outgoing SIP MESSAGE request MIME bodies as specified in subclause 6.3.2.2.9; and

4) shall copy the contents of the P-Asserted-Identity header field of the incoming SIP MESSAGE request to the P-Asserted-Identity header field of the outgoing SIP MESSAGE request.

6.3.2.3 Void

6.3.3 Controlling MCPTT function

6.3.3.1 Request initiated by the controlling MCPTT function

6.3.3.1.1 SDP offer generation

The SDP offer is generated based on the received SDP offer. The SDP offer generated by the controlling MCPTT function:

1) when initiating a new MCPTT session the SDP offer;

   a) shall contain only one SDP media-level section for MCPTT speech media stream as contained in the received SDP offer; and

   b) shall contain an SDP media-level section for one media-floor control entity, if present in the received SDP offer; and

2) when adding a new MCPTT user to an existing MCPTT Session, the SDP offer shall contain the media stream currently used in the MCPTT session.

When composing the SDP offer according to 3GPP TS 24.229 [4], the controlling MCPTT function:

1) shall replace the IP address and port number for the offered media stream in the received SDP offer with the IP address and port number of the controlling MCPTT function;

2) for the MCPTT speech media stream, shall include all media-level attributes from the received SDP offer;

3) shall replace the IP address and port number for the offered media floor control entity, if any, in the received SDP offer with the IP address and port number of the controlling MCPTT function; and

4) for the offered media floor control entity, shall include the offered media floor control entity 'fmtp' attributes as specified in 3GPP TS 24.380 [5] clause 14.

6.3.3.1.2 Sending an INVITE request

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) if the received SIP INVITE request contained an application/vnd.3gpp.mcptt-info+xml MIME body containing an <ambient-listening-type> element and:

   a) if the Priv-Answer-Mode header field specified in IETF RFC 5373 [18] was included in the received SIP INVITE request with a value of "Auto" or if no Priv-Answer-Mode header field was received in the received SIP INVITE request; or

   b) a Priv-Answer-Mode header field was received containing a value other than "Auto";

   shall include a Priv-Answer-Mode header field set to a value of "Auto" in the outgoing SIP INVITE request;

9) if the received SIP INVITE request did not contain an application/vnd.3gpp.mcptt-info+xml MIME body containing an <ambient-listening-type> element, 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.

6.3.3.1.3 Receipt of a SIP response to a SIP INVITE request

6.3.3.1.3.1 Final response

On receipt of the SIP 200 (OK) response to the initial outgoing SIP INVITE request the controlling MCPTT function:

1) shall start the SIP session timer according to rules and procedures of IETF RFC 4028 [7]; and

2) shall cache SIP feature tags, if received in the Contact header field, and if the specific feature tags are supported.

6.3.3.1.4 Void

6.3.3.1.5 Sending a SIP BYE request

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.

6.3.3.1.6 Sending a SIP re-INVITE request for MCPTT emergency group call

This subclause is referenced from other procedures.

The controlling MCPTT function shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [4].

The controlling MCPTT function:

1) shall include an SDP offer with the media parameters as currently established with the terminating MCPTT client according to 3GPP TS 24.229 [4];

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcptt-calling-user-id> element set to the MCPTT ID of the initiating MCPTT user;

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

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

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

   c) if the <alert-ind> element is set to "true" in the received SIP re-INVITE request and MCPTT emergency alerts are authorised for this group and MCPTT user 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 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" in the application/vnd.3gpp.mcptt-info+xml MIME body; and

   d) 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"; and

NOTE: If the imminent peril state of the group is true at this point, the controlling function will be setting it to false as part of the calling procedure. This is in effect an upgrade of an MCPTT imminent peril group call to an MCPTT emergency group call.

4) if the in-progress emergency group state of the group is set to a value of "false":

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

   b) if the received SIP re-INVITE request contained an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "false" and this is an authorised request to cancel an MCPTT emergency group call as determined by the procedures of subclause 6.3.3.1.13.4:

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

      ii) if the received SIP re-INVITE request contained an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "false" and this is an authorised request to cancel an MCPTT emergency alert as determined by the procedures of subclause 6.3.3.1.15, shall:

         A) include in the application/vnd.3gpp.mcptt-info+xml MIME body an <alert-ind> element set to a value of "false"; and

         B) if the received SIP request contains an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, copy the contents of the received <originated-by> element to an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP re-INVITE request.

6.3.3.1.7 Sending a SIP INVITE request for MCPTT emergency group call

This subclause is referenced from other procedures.

This subclause describes the procedures for inviting an MCPTT user to an MCPTT session associated with an MCPTT emergency group call or MCPTT imminent peril group call. The procedure is initiated by the controlling MCPTT function as the result of an action in subclause 10.1.2.4.1.1.

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 address of the terminating participating MCPTT function associated with the MCPTT ID of the targeted MCPTT user;

3) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element populated as follows:

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

   b) the <mcptt-calling-user-id> element set to the value of the MCPTT ID of the calling MCPTT user; and

   c) the <mcptt-calling-group-id> element set to the value of the MCPTT group ID of the emergency group call.

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

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; and

6) if the in-progress emergency group 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) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <emergency-ind> element set to a value of "true";

   c) 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" in the application/vnd.3gpp.mcptt-info+xml MIME body; and

   d) 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";

NOTE: If the imminent peril state of the group is true at this point, the controlling function will set it to false as part of the calling procedure.

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".

6.3.3.1.8 Sending a SIP UPDATE request for Resource-Priority header field correction

This subclause is referenced from other procedures.

This subclause describes the procedures for updating an MCPTT session associated with an MCPTT emergency group call or MCPTT imminent peril group call when the received SIP INVITE request did not include a correctly populated

Resource-Priority header field. The procedure is initiated by the controlling MCPTT function for the purpose of providing the correct Resource-Priority header field.

1) shall generate a SIP 183 (Session Progress) response according to 3GPP TS 24.229 [4] with the clarifications provided specified in subclause 6.3.3.2.3.1;

2) shall include the option tag "100rel" in a Require header field in the SIP 183 (Session Progress) response;

3) shall include in the SIP 183 (Session Progress) response an SDP answer to the SDP offer in the incoming SIP INVITE request as specified in the subclause 6.3.3.2.1; and

4) shall send the SIP 183 (Session Progress) response towards the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP PRACK request to the SIP 183 (Session Progress) response the controlling MCPTT function:

1) shall send the SIP 200 (OK) response to the SIP PRACK request according to 3GPP TS 24.229 [4].

2) shall generate a SIP UPDATE request according to 3GPP TS 24.229 [4] with the following clarifications:

3) shall include in the SIP UPDATE 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;

4) if the in-progress emergency group state of the group is set to a value of "true" the controlling MCPTT function shall include a Resource-Priority header field populated for an MCPTT emergency group call as specified in subclause 6.3.3.1.19; and

NOTE 1: This is the case when the sending MCPTT client did not send a Resource-Priority header field populated appropriately to receive emergency-level priority. In this case, the Resource-Priority header field is populated appropriately to provide emergency-level priority.

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

   a) if the in-progress imminent peril state of the group is set to a value of "false", shall include a Resource-Priority header field populated for a normal priority MCPTT group call as specified in subclause 6.3.3.1.19; and

   b) if the in-progress imminent peril state of the group is set to a value of "true", shall include a Resource-Priority header field populated for an MCPTT imminent peril group call as specified in subclause 6.3.3.1.19.

NOTE 2: This is the case when the sending MCPTT client incorrectly populated a Resource-Priority header field for emergency-level or imminent peril-level priority and the controlling MCPTT function re-populates it as appropriate to an imminent peril level priority or normal priority level.

6.3.3.1.9 Generating a SIP re-INVITE request

This subclause is referenced from other procedures.

This subclause describes the procedures for generating a SIP re-INVITE request to be sent by the controlling MCPTT function.

The controlling MCPTT function:

1) shall generate an SIP re-INVITE request according to 3GPP TS 24.229 [4]; and

2) shall include an SDP offer with the media parameters as currently established with the terminating MCPTT client according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.3.3.1.1.

6.3.3.1.10 Generating a SIP re-INVITE request to cancel an in-progress emergency

This subclause is referenced from other procedures.

This subclause describes the procedures for generating a SIP re-INVITE request to cancel the in-progress emergency state of an MCPTT group. The procedure is initiated by the controlling MCPTT function when it determines the cancellation of the in-progress emergency state of an MCPTT group is required.

The controlling MCPTT function:

1) shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.3.3.1.9;

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

3) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "false".

6.3.3.1.11 Generating a SIP MESSAGE request for notification of in-progress emergency or imminent peril status change

This subclause is referenced from other procedures.

This subclause describes the procedures for generating a SIP MESSAGE request to notify affiliated but not participating members of an MCPTT group of the change of status of the in-progress emergency state, imminent peril state or emergency alert status of an MCPTT group. The procedure is initiated by the controlling MCPTT function when there has been a change of in-progress imminent peril, in-progress emergency or the emergency alert status of an MCPTT group.

The controlling MCPTT function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

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 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];

4) shall set the Request-URI to the address of the terminating participating function associated with the MCPTT ID of the targeted MCPTT user;

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

6) 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];

7) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <mcptt-request-uri> element set to the value of the MCPTT ID of the targeted MCPTT user; and

8) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <mcptt-calling-group-id> element set to the MCPTT group ID of the MCPTT group on which the MCPTT emergency call, imminent peril call or the emergency alert state has changed.

6.3.3.1.12 Populate mcptt-info and location-info MIME bodies for emergency alert

This subclause is referenced from other procedures.

This subclause describes the procedures for populating the application/vnd.3gpp.mcptt-info+xml and application/vnd.3gpp.mcptt-location-info+xml MIME bodies for an MCPTT emergency alert. The procedure is initiated by the controlling MCPTT function when it has received a SIP request initiating an MCPTT emergency alert and generates a message containing the MCPTT emergency alert information required by 3GPP TS 23.379 [3].

The controlling MCPTT function:

1) shall include, if not already present, an application/vnd.3gpp.mcptt-info+xml MIME body as specified in Annex F.1, and set the <alert-ind> element to a value of "true";

2) shall determine the value of the MCPTT user's Mission Critical Organization from the <MissionCriticalOrganization> element, of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]);

3) shall include in the <mcpttinfo> element containing the <mcptt-Params> element containing an <mc-org> element set to the value of the MCPTT user's Mission Critical Organization; and

4) shall copy the contents of the application/vnd.3gpp.mcptt-location-info+xml MIME body in the received SIP request into an application/vnd.3gpp.mcptt-location-info+xml MIME body included in the outgoing SIP request.

6.3.3.1.13 Authorisations

6.3.3.1.13.1 Determining authorisation for initiating an MCPTT emergency alert

If the controlling MCPTT function has received a SIP request targeted to an MCPTT group with the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "true", the controlling MCPTT function shall check the following conditions:

1) if the <allow-activate-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true";

   a) if the "entry-info" attribute of the <entry> element of the <EmergencyAlert> element contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "DedicatedGroup" and:

      i) if the MCPTT group identity targeted for the emergency alert is contained in the <uri-entry> element of the <entry> element of the <EmergencyAlert> element contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]); and

      ii) if the <allow-MCPTT-emergency-alert> element of the <list-element> of the group document identified by the MCPTT group identity is set to a value of "true" as specified in 3GPP TS 24.481 [31]; or

   b) if the "entry-info" attribute of the <entry> element of the <EmergencyAlert> element contained within the <MCPTT-group-call> element of the MCPTT user profile (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UseCurrentlySelectedGroup" and the <allow-MCPTT-emergency-alert> element of the <list-element> of the group document identified by the MCPTT group identity targeted for the emergency alert is set to a value of "true" as specified in 3GPP TS 24.481 [31].

then the MCPTT emergency alert request shall be considered to be an authorised request for an MCPTT emergency alert targeted to a MCPTT group. In all other cases, the MCPTT emergency alert request shall be considered to be an unauthorised request for an MCPTT emergency alert targeted to an MCPTT group.

If the controlling MCPTT function has received a SIP request targeted to an MCPTT user with the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "true", the controlling MCPTT function shall check the following conditions:

1) if the <allow-activate-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true"; and

   a) if the "entry-info" attribute of the <entry> element of the <PrivateEmergencyAlert> element contained within the <OnNetwork> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UsePreConfigured" and the MCPTT ID of the MCPTT user targeted for the call is contained in the <uri-entry> element of the <entry> element of the <PrivateEmergencyAlert> element contained within the <OnNetwork> element (see the MCPTT user profile document in 3GPP TS 24.484 [50]); or

   b) if the "entry-info" attribute of the <entry> element of the <PrivateEmergencyAlert> element contained within the <OnNetwork> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "LocallyDetermined";

then the MCPTT emergency alert request shall be considered to be an authorised request for an MCPTT emergency alert targeted to an MCPTT user. In all other cases, it shall be considered to be an unauthorised request for an MCPTT emergency alert targeted to an MCPTT user.

6.3.3.1.13.2 Determining authorisation for initiating an MCPTT emergency group or private call

If the controlling MCPTT function has received a SIP request for an MCPTT group call with the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "true" and:

1) if the <allow-emergency-group-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true" and:

   a) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> element contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "DedicatedGroup" and:

      i) if the <uri-entry> element of the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) contains the identity of the MCPTT group targeted by the calling MCPTT user; and

      ii) if the <allow-MCPTT-emergency-call> element of the <list-service> element of the group document identified by the targeted MCPTT group identity is set to a value of "true" as specified in 3GPP TS 24.481 [31];

   then the controlling MCPTT function shall consider the MCPTT emergency group call request to be an authorised request for an MCPTT emergency group call and skip the remaining steps; or;

   b) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element of the <EmergencyCall> element contained within the <MCPTT-group-call> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UseCurrentlySelectedGroup" and if the <allow-MCPTT-emergency-call> element of the <list-service> element of the group document identified by the targeted MCPTT group identity is set to a value of "true" as specified in 3GPP TS 24.481 [31];

   then the controlling MCPTT function shall consider the MCPTT emergency group call request to be an authorised request for an MCPTT emergency group call and skip the remaining steps; or

2) if the controlling MCPTT function does not consider the MCPTT emergency group call request to be an authorised request for an MCPTT emergency group call by step 1) above, then the controlling MCPTT function shall consider the MCPTT emergency group call request to be an unauthorised request for an MCPTT emergency group call.

If the controlling MCPTT function has received a SIP request for an MCPTT private call with the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "true" and:

1) if the <allow-emergency-private-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true"; and

   a) if the "entry-info" attribute of the <entry> element of the <MCPTTPrivateRecipient> element of the <EmergencyCall> element contained within the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UsePreConfigured" and if the MCPTT ID targeted for the call is contained in the <uri-entry> element of the <entry> element of the <MCPTTPrivateRecipient> element of the <EmergencyCall> element contained within the <PrivateCall> element (see the MCPTT user profile document in 3GPP TS 24.484 [50]); or

   b) if the "entry-info" attribute of the <entry> element of the <MCPTTPrivateRecipient> element of the <EmergencyCall> element contained within the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "LocallyDetermined";

   then the controlling MCPTT function shall consider the MCPTT emergency private call request to be an authorised request for an MCPTT emergency private call and skip step 2) below; or

2) if the controlling MCPTT function does not consider the MCPTT emergency private call request to be an authorised request for an MCPTT emergency private call by step 1) above, then the controlling MCPTT function

shall consider the MCPTT emergency private call request to be an unauthorised request for an MCPTT emergency private call.

6.3.3.1.13.3 Determining authorisation for cancelling an MCPTT emergency alert

If the controlling MCPTT function has received a SIP request with the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "false" and:

1) if the <allow-cancel-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true", then the MCPTT emergency alert cancellation request shall be considered to be an authorised request for an MCPTT emergency alert cancellation; and

2) if the <allow-cancel-emergency-alert> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "false", then the MCPTT emergency alert cancellation request shall be considered to be an unauthorised request for an MCPTT emergency alert cancellation.

6.3.3.1.13.4 Determining authorisation for cancelling an MCPTT emergency call

If the controlling MCPTT function has received a SIP request for an MCPTT group call with the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "false" and:

1) if the <allow-cancel-group-emergency> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true", then the MCPTT emergency call cancellation request shall be considered to be an authorised request for an MCPTT emergency group call cancellation; and

2) If the <allow-cancel-group-emergency> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "false", then the MCPTT emergency group call cancellation request shall be considered to be an unauthorised request for an MCPTT emergency group call cancellation.

If the controlling MCPTT function has received a SIP request for an MCPTT private call with the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "false" and:

1) if the <allow-cancel-private-emergency-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true", then the MCPTT emergency private call cancellation request shall be considered to be an authorised request for an MCPTT emergency private call cancellation; and

2) if the <allow-cancel-private-emergency-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "false" or not present, then the MCPTT emergency private call cancellation request shall be considered to be an unauthorised request for an MCPTT emergency private call cancellation.

6.3.3.1.13.5 Determining authorisation for initiating an MCPTT imminent peril call

If the controlling MCPTT function has received a SIP request with the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "true" and:

1) if the <allow-imminent-peril-call> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value other than "true" the request for initiating an MCPTT imminent peril call shall be considered to be an unauthorised request for an MCPTT imminent peril call and skip the remaining steps;

2) if the <allow-imminent-peril-call> element of the <list-service> element of the group document identified by the targeted MCPTT group identity is set to a value other than "true" as specified in 3GPP TS 24.481 [31], the request for initiating an MCPTT imminent peril call shall be considered to be an unauthorised request for an MCPTT imminent peril call and skip the remaining steps;

3) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element contained within the <ImminentPerilCall> element of the MCPTT user profile document (see the MCPTT user profile document

in 3GPP TS 24.484 [50]) is set to a value of "DedicatedGroup" and if the MCPTT group identity targeted for the call is contained in the <uri-entry> element of the <entry> element of the <MCPTTGroupInitiation> element contained within the <ImminentPerilCall> element (see the MCPTT user profile document in 3GPP TS 24.484 [50]); or

4) if the "entry-info" attribute of the <entry> element of the <MCPTTGroupInitiation> element contained within the <ImminentPerilCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "UseCurrentlySelectedGroup".

then the MCPTT imminent peril call request shall be considered to be an authorised request for an MCPTT imminent peril call. In all other cases, it shall be considered to be an unauthorised request for an MCPTT imminent peril call.

6.3.3.1.13.6 Determining authorisation for cancelling an MCPTT imminent peril call

If the controlling MCPTT function has received a SIP request with the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "false" and:

1) if the <allow-cancel-imminent-peril> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "true", then the MCPTT emergency call cancellation request shall be considered to be an authorised request for an MCPTT imminent peril call cancellation; and

2) if the <allow-cancel-imminent-peril> element of the <ruleset> element of the MCPTT user profile document identified by the MCPTT ID of the calling user (see the MCPTT user profile document in 3GPP TS 24.484 [50]) is set to a value of "false" or not present, then the MCPTT emergency call cancellation request shall be considered to be an unauthorised request for an MCPTT imminent peril call cancellation.

6.3.3.1.13.7 Sending a SIP OPTIONS request to authorise an MCPTT user at a non-controlling MCPTT function of a MCPTT group

This subclause is referenced from other procedures.

The controlling MCPTT function:

1) if the <associated-group-id> element is included in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request, shall generate a SIP OPTIONS request according to 3GPP TS 24.229 [4] and the IETF RFC 3261 [24] populated as follows:

   a) shall set the Request-URI to the public service identity of the non-controlling MCPTT function associated with the MCPTT Group ID which was present in the <associated-group-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request;

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

   b) 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];

   c) shall include in the P-Asserted-Identity header field, the public service identity of the controlling MCPTT function;

   d) shall include an application/vnd.3gpp.mcptt-info+xml MIME body where:

      i) the <mcptt-request-uri> element shall be set to the value of the <associated-group-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request; and

      ii) the <mcptt-calling-user-id> element is set to the same value as in the <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request;

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

      i) the g.3gpp.mcptt media feature tag; and

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

f) send the SIP OPTIONS request as specified in 3GPP TS 24.229 [4]; and

2) if the <associated-group-id> element is not included in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request, shall for each constituent MCPTT group ID in the <constituent-MCPTT-group-ID> element not homed at the controlling MCPTT function generate a SIP OPTIONS request according to 3GPP TS 24.229 [4] and IETF RFC 3261 [24] populated as follows:

a) shall set the Request-URI to the public service identity of the non-controlling MCPTT function associated with the MCPTT group ID in the <constituent-MCPTT-group-ID> element;

NOTE 2: How the controlling MCPTT function finds the address of the non-controlling MCPTT function is out of the scope of the current release.

b) 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];

c) shall include in the P-Asserted-Identity header field, the public service identity of the controlling MCPTT function;

d) shall include an application/vnd.3gpp.mcptt-info+xml MIME body where:

i) the <mcptt-request-uri> element shall be set to the MCPTT group ID in the <constituent-MCPTT-group-ID> element; and

ii) the <mcptt-calling-user-id> element is set to the same value as in the <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request;

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

i) the g.3gpp.mcptt media feature tag; and

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

f) send the SIP OPTIONS request as specified in 3GPP TS 24.229 [4].

Upon receipt of the first SIP 200 (OK) response to the SIP OPTIONS request with the mcptt-warn-code set to "147" in a Warning header field as specified in subclause 4.4, the controlling MCPTT function shall return a SIP 302 (Moved Temporarily) response to the "SIP INVITE request for controlling MCPTT function of an MCPTT group" populated as follows:

1) the URI in the Contact header field set to the P-Asserted-Identity received in the SIP 200 (OK) response;

2) an application/vnd.3gpp.mcptt-info MIME body with:

a) the <mcptt-request-uri> element set to the same value as received in the <mcptt-request-uri> in the SIP 2xx response to the SIP OPTIONS request; and

b) the <session-type> element set to the value received in the <session-type> element in the appication/vnd.3gpp.mcptt.info+xml MIME body of the received SIP 2xx response to the SIP OPTIONS request; and

3) if more than one OPTIONS request were sent, shall remove any cached SIP response and ignore any other responses to any other OPTIONS request.

Upon receipt of a SIP 404 (Not Found) response to the SIP OPTIONS request such that the mcptt-warn-code set to "113" in a Warning header field as specified in subclause 4.4, the controlling MCPTT function:

1) if more than one SIP OPTIONS request were sent and if no other responses to SIP OPTIONS request are expected; shall send a SIP 404 (Not Found) response to "SIP INVITE request for controlling MCPTT function of an MCPTT group" and include the Warning header field received in the SIP 404 (Not Found) response; and

2) if more than one OPTIONS request were sent and other responses to SIP OPTIONS request are expected, shall cache the received SIP 404 (Not Found) response.

Upon receipt of a SIP 403 (Forbidden) response to the SIP OPTIONS request, the mcptt-warn-code set to "106" or "109" in a Warning header field as specified in subclause 4.4 and if more than one OPTIONS request were sent and if no other responses to the SIP OPTIONS request are expected, the controlling MCPTT function:

1) if a SIP 404 (Not Found) response is cached, send a SIP 404 (Not Found) response to "SIP INVITE request for controlling MCPTT function of an MCPTT group" and include the Warning header field received in the SIP 404 (Not Found) response; and

2) if a SIP 404 (Not Found) response is not cached, shall return a SIP 403 (Forbidden) response to "SIP INVITE request for controlling MCPTT function of an MCPTT group" and include the Warning header field received in the SIP 403 (Forbidden) response.

Upon receipt of any other response to the SIP OPTIONS response than specified above and if more than one OPTIONS request were sent and if no other responses to the SIP OPTIONS request are expected, the controlling MCPTT function:

1) if a SIP 404 (Not Found) response is cached, send a SIP 404 (Not Found) response to "SIP INVITE request for controlling MCPTT function of an MCPTT group" and include the Warning header field received in the SIP 404 (Not Found) response; and

2) if a SIP 404 (Not Found) response is not cached, shall return a SIP 403 (Forbidden) response to "SIP INVITE request for controlling MCPTT function of an MCPTT group".

NOTE 3: The reason for selecting the SIP 404 (Not Found) response when a SIP 404 (Not Founf) response is cached is to indicate that it was a valid request but the MCPTT user identified in the <mcptt-calling-user-id> is not a member of any of the constituent MCPTT groups in the temporary group document.

6.3.3.1.14 Generating a SIP 403 response for priority call request rejection

If the controlling MCPTT function has received a SIP request with the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body is set to "true" and this is an unauthorised request for an MCPTT emergency call as determined by the procedures of subclause 6.3.3.1.13.2, the controlling MCPTT function shall:

1) include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in Annex F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "false" and the <alert-ind> element set to a value of "false".

6.3.3.1.15 Sending a SIP re-INVITE request for MCPTT imminent peril group call

This subclause is referenced from other procedures.

The controlling MCPTT function shall generate a SIP re-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 and the isfocus media feature tag according to IETF RFC 3840 [16];

2) shall include an SDP offer with the media parameters as currently established with the terminating MCPTT client according to 3GPP TS 24.229 [4];

3) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcptt-calling-user-id> element set to the MCPTT ID of the initiating MCPTT user;

4) if 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 an <imminentperil-ind> element set to a value of "true"; and

5) if the in-progress imminent peril state of the group is set to a value of "false":

   a) shall include a Resource-Priority header field populated with the values for a normal MCPTT 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 an <emergency-ind> element set to a value of "false" and the <imminentperil-ind> element set to a value of "false".

6.3.3.1.16 Handling the expiry of timer TNG2 (in-progress emergency group call timer)

Upon expiry of timer TNG2 (in-progress emergency group call timer) for an MCPTT group, the controlling MCPTT function:

1) shall set the in-progress emergency state of the group to a value of "false";

2) shall, if an MCPTT group call or MCPTT group session is in progress on the indicated group, for each of the participating members:

   a) generate a SIP re-INVITE request as specified in subclause 6.3.3.1.10; and

   b) send the SIP re-INVITE request towards the MCPTT client according to 3GPP TS 24.229 [4]; and

3) shall for each affiliated but non-participating members member of the group:

   a) generate a SIP MESSAGE request according to subclause 6.3.3.1.11 and include in the application/vnd.3gpp.mcptt-info+xml MIME body an <emergency-ind> element set to a value of "false";

   b) shall include in the P-Asserted-Identity header field the public service identity of the controlling MCPTT function;

   c) 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]; and

   d) send the SIP MESSAGE request towards the MCPTT client according to rules and procedures of 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to a re-SIP INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5].

6.3.3.1.17 Validate priority request parameters

This subclause is referenced from other procedures. This procedure validates the combinations of <emergency-ind>, <imminentperil-ind> and <alert-ind> in the application/vnd.3gpp.mcptt-info+xml MIME body included in:

1) a SIP INVITE request or SIP re-INVITE request; or

2) the body "URI" header field of the SIP URI included in the application/resource-lists MIME body which is pointed to by a "cid" URL located in the Refer-To header of a SIP REFER request;

Upon receiving a SIP request as specified above with the <emergency-ind> element set to a value of "true", the controlling MCPTT function shall only consider the following as valid combinations:

1) <imminentperil-ind> not included and <alert-ind> included.

Upon receiving a SIP request as specified above with the <emergency-ind> element set to a value of "false", the controlling MCPTT function shall only consider the following as valid combinations:

1) <imminentperil-ind> not included and <alert-ind> not included; or

2) <imminentperil-ind> not included and <alert-ind> included.

Upon receiving a SIP request as specified above with the <imminentperil-ind> element included the controlling MCPTT function shall only consider the request as valid if both the <emergency-ind> and <alert-ind> are not included.

If the combination of the <emergency-ind>, <imminentperil-ind> or <alert-ind> indicators is invalid, the controlling MCPTT function shall send a SIP 403 (Forbidden) response with the warning text set to "150 invalid combinations of data received in MIME body" in a Warning header field as specified in subclause 4.4.

6.3.3.1.18 Sending a SIP INFO request in the dialog of a SIP request for a priority call

This subclause is referenced from other procedures and describes how the controlling MCPTT function generates a SIP INFO request due to the receipt of a SIP request for a priority call.

The controlling MCPTT function:

1) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [4] and IETF RFC 6086 [64];

2) shall include the Info-Package header field set to g.3gpp.mcptt-info in the SIP INFO request;

3) shall include an application/vnd.3gpp.mcptt-info+xml MIME body in the SIP INFO request and:

   a) if the received SIP request contained application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall set the <emergency-ind> element to a value of "true" and the <alert-ind> element to a value of "false";

   b) if the received SIP request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "false" and if this is an unauthorised request for an MCPTT emergency alert cancellation, shall set <alert-ind> element to a value of "true"; and

   c) if the received SIP request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "true", this is an authorised request for an MCPTT imminent peril group call and the in-progress emergency state of the group is set to a value of "true", shall set the <imminentperil-ind> element to a value of "false" and the <emergency-ind> element set to a value of "true"; and

4) shall send the SIP INFO request towards the inviting MCPTT client in the dialog created by the SIP request from the inviting MCPTT client, as specified in 3GPP TS 24.229 [4].

6.3.3.1.19 Retrieving Resource-Priority header field values

This subclause is referenced from other procedures.

When determining the Resource-Priority header field namespace and priority values as specified in IETF RFC 8101 [48] for an MCPTT emergency group call or MCPTT emergency private call the controlling MCPTT function:

1) shall retrieve the value of the <resource-priority-namespace> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]); and

2) shall retrieve the value of the <resource-priority-priority> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]).

When determining the Resource-Priority header field namespace and priority values as specified in IETF RFC 8101 [48] for an MCPTT imminent peril group call the controlling MCPTT function:

1) shall retrieve the value of the <resource-priority-namespace> element contained in the <imminent-peril-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]); and

2) shall retrieve the value of the <resource-priority-priority> element contained in the <imminent-peril-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50])

When determining the Resource-Priority header field namespace and priority values as specified in IETF RFC 8101 [48] for a normal MCPTT group or private call the controlling MCPTT function:

1) shall retrieve the value of the <resource-priority-namespace> element contained in the <normal-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]); and

2) shall retrieve the value of the <resource-priority-priority> element contained in the <normal-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document (see the service configuration document in 3GPP TS 24.484 [50]).

NOTE: The "normal" Resource-Priority header field value is needed to return to a normal priority value from a priority value adjusted for an MCPTT emergency group or private call or an MCPTT imminent peril group call. The "normal" priority received from the EPS by use of the "normal" Resource-Priority header field value is expected to be the same as the "normal" priority received from the EPS when initiating a call with no Resource-Priority header field included.

6.3.3.1.20 Generating a SIP MESSAGE request to indicate successful receipt of an emergency alert or emergency cancellation

This subclause is referenced from other procedures.

This subclause describes the procedures for generating a SIP MESSAGE request to notify the originator of an emergency alert or emergency cancellation that the request was successfully received.

The controlling MCPTT function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

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 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];

4) shall set the Request-URI to the address of the terminating participating function associated with the MCPTT ID of the targeted MCPTT user;

5) shall include a P-Asserted-Identity header field set to the public service identity of controlling MCPTT function; and

6) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <mcptt-request-uri> element set to the value of the MCPTT ID of the targeted MCPTT user.

6.3.3.2 Requests terminated by the controlling MCPTT function

6.3.3.2.1 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [4], the controlling MCPTT function:

1) for the accepted media stream in the received SDP offer:

   a) shall replace the IP address and port number in the received SDP offer with the IP address and port number of the controlling MCPTT function; and

2) for the accepted media-floor control entity, if present in the received SDP offer:

   a) shall replace the IP address and port number in the received SDP offer with the IP address and port number of the controlling MCPTT function, for the accepted media-floor control entity, if present in the received SDP offer; and

   b) shall include 'fmtp' attributes as specified in 3GPP TS 24.380 clause 14.

6.3.3.2.2 Receipt of a SIP INVITE request

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.

6.3.3.2.3 Sending a SIP response to a SIP INVITE request

6.3.3.2.3.1 Provisional response

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.

6.3.3.2.3.2 Final response

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

6.3.3.2.4 Receiving a SIP BYE request

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:

   a) shall perform the procedures as specified in the subclause 6.3.3.1.5 with the clarification that if the received SIP BYE request contains an application/vnd.3gpp.mcptt-info+xml MIME body, copy the application/vnd.3gpp.mcptt-info+xml MIME body into the outgoing SIP BYE request; 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.

6.3.3.3 Handling of the acknowledged call setup timer (TNG1)

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 24.481 [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.

After expiry of timer TNG1 (acknowledged call setup timer) and the local counter of the number of SIP 200 (OK) responses received from invited members is less than the value of the <on-network-minimum-number-to-start> element of the group document, then the controlling MCPTT function shall wait until further responses have been received from invited clients and the value of the local counter of the number of SIP 200 (OK) responses received from invited members is equal to the <on-network-minimum-number-to-start>, before continuing with the timer TNG1 expiry procedures in this subclause.

After expiry of timer TNG1 (acknowledged call setup timer) and the local counter of the number of SIP 200 (OK) responses received from invited members is greater or equal to the value of the <on-network-minimum-number-to-start> element of the group document, the controlling MCPTT function shall execute the steps described below:

1) if the <on-network-action-upon-expiration-of-timeout-for-acknowledgement-of-required-members> element configured in the group document for the action on expiry of the timer is set to "proceed" indicating that the controlling MCPTT function should proceed with the setup of the group call, then the controlling MCPTT function:

   a) shall perform the following actions:

      i) generate a SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.3.2.2 before continuing with the rest of the steps;

ii) include in the SIP 200 (OK) response the warning text set to "111 group call proceeded without all required group members" in a Warning header field as specified in subclause 4.4;

iii) 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;

iv) interact with the media plane as specified in 3GPP TS 24.380 [5]; and

NOTE 2: Resulting media plane processing is completed before the next step is performed.

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

b) when a SIP 200 (OK) response to a SIP INVITE request is received from an invited MCPTT client the controlling MCPTT function may send an in-dialog SIP MESSAGE request to the MCPTT client that originated the group session with the text "group call proceeded without all required group members";

c) when the controlling MCPTT function receives a SIP BYE request from an invited MCPTT client, shall take the actions specified in subclause 6.3.3.2.4 and may send an in-dialog SIP MESSAGE request to the MCPTT client that originated the group session with the text "group call proceeded without all required group members"; and

d) shall generate a notification package as specified in subclause 6.3.3.4 and send a SIP NOTIFY request according to 3GPP TS 24.229 [4] to the MCPTT clients which have subscribed to the conference state event; and

2) if the <on-network-action-upon-expiration-of-timeout-for-acknowledgement-of-required-members> element configured in the group document for the action on expiry of the timer is set to "abandon" indicating that the controlling MCPTT function should abandon the setup of the group call, then the controlling MCPTT function shall:

a) send a SIP 480 (Temporarily Unavailable) response to the MCPTT client that originated the group session with the warning text set to "112 group call abandoned due to required group members not part of the group session" in a Warning header field as specified in subclause 4.4;

b) for each confirmed dialog at the controlling MCPTT function, send a SIP BYE request towards the MCPTT clients invited to the group session in accordance with 3GPP TS 24.229 [4] and interact with the media plane as specified in 3GPP TS 24.380 [5]; and

c) for each non-confirmed dialog at the controlling MCPTT function, send a SIP CANCEL request towards the MCPTT clients invited to the group session in accordance with 3GPP TS 24.229 [4].

If the controlling MCPTT function receives a final SIP 4xx, 5xx or 6xx response from an affiliated and <on-network-required> group member prior to expiry of timer TNG1 (acknowledged call setup timer) and based on policy, the controlling MCPTT function decides not to continue with the establishment of the group call without the affiliated and <on-network-required> group member, then the controlling MCPTT function:

NOTE 3: It is expected that this action is taken if the policy is to abandon the call on expiry of timer TNG1 (acknowledged call setup timer).

1) shall stop timer TNG1 (acknowledged call setup timer); and

2) shall forward the final SIP 4xx, 5xx or 6xx response towards the inviting MCPTT client with the warning text set to "112 group call abandoned due to required group member not part of the group session" in a Warning header field as specified in subclause 4.4.

If:

1) the controlling MCPTT function receives a final SIP 4xx, 5xx or 6xx response from an affiliated and <on-network-required> group member prior to expiry of timer TNG1 (acknowledged call setup timer);

2) 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; and

3) based on policy, the controlling MCPTT function decides to continue with the establishment of the group call without the affiliated and <on-network-required> group member;

then the controlling MCPTT function:

NOTE 4: It is expected that this action is taken if the policy is to proceed with the call on expiry of timer TNG1 (acknowledged call setup timer).

1) if all other invited clients have not yet responded, shall continue running timer TNG1 (acknowledged call setup timer); and

2) if all other invited clients have responded with SIP 200 (OK) responses, shall

   a) stop timer TNG1 (acknowledged call setup timer);

   b) generate SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.3.2.2 before continuing with the rest of the steps;

   c) include in the SIP 200 (OK) response the warning text set to "111 group call proceeded without all required group members" in a Warning header field as specified in subclause 4.4;

   d) 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;

   e) interact with the media plane as specified in 3GPP TS 24.380 [5]; and

NOTE 5: Resulting media plane processing is completed before the next step is performed.

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

6.3.3.4 Generating a SIP NOTIFY request

The controlling MCPTT function shall generate a SIP NOTIFY request according to 3GPP TS 24.229 [4] with the clarification in this subclause.

In the SIP NOTIFY request, the controlling MCPTT function:

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

2) shall include an Event header field set to the “conference” event package;

3) shall include an Expires header field set to 3600 seconds according to IETF RFC 4575 [30], as default value;

4) 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-Preferred-Service header field according to IETF RFC 6050 [9]; and

5) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with:

   a) the <mcptt-calling-group-id> set to the value of the MCPTT group ID;

   b) if the target is a MCPTT user, the value of <mcptt-request-uri> element set to the value of MCPTT ID of the targeted MCPTT user; and

   c) if the target is the non-controlling MCPTT function, the value of <mcptt-request-uri> element set to the constituent MCPTT group ID.

In the SIP NOTIFY request, the controlling MCPTT function shall include an application/conference-info+xml MIME body according to IETF RFC 4575 [30] with the following limitations:

1) the controlling MCPTT function shall include the MCPTT group ID of the MCPTT group in the "entity" attribute of the <conference-info> element;

2) for each participant in the MCPTT session with the exception of non-controlling MCPTT functions, the controlling MCPTT function shall include a <user> element. The <user> element shall:

NOTE: Non-controlling MCPTT functions will appear as a participant in temporary group sessions.

   a) include the "entity" attribute. The "entity" attribute:

i) shall for the MCPTT client, which initiated, joined or re-joined an MCPTT session, include the MCPTT ID of the MCPTT user which originates SIP INVITE request; and

ii) shall for an invited MCPTT client include the MCPTT ID of the invited MCPTT user in case of a prearranged group call or chat group call;

b) shall include a single <endpoint> element. The <endpoint> element:

i) shall include the "entity" attribute; and

ii) shall include the <status> element indicating the status of the MCPTT session according to RFC 4575; and

c) may include <roles> element.

NOTE: The usage of <roles> is only applicable for human consumption.

6.3.3.5 Handling of the group call timer (TNG3)

6.3.3.5.1 General

When the controlling MCPTT function receives a SIP INVITE request to initiate a group session, then after an MCPTT session identity has been allocated for the group session and if the <on-network-maximum-duration> element is present in the group document as specified in 3GPP TS 24.481 [31], the controlling MCPTT function: shall start timer TNG3 (group call timer) with the value obtained from the <on-network-maximum-duration> element of the group document as specified in 3GPP TS 24.481 [31].

If the <on-network-maximum-duration> element is not present in the group document as specified in 3GPP TS 24.481 [31], then the controlling MCPTT function shall not start timer TNG3 (group call timer).

NOTE 1: The configuration of <on-network-maximum-duration> element in 3GPP TS 24.481 [31] is mandated for a pre-arranged group and is optional for a chat group.

When merging two or more active group calls into a temporary group call, the controlling MCPTT function(s) hosting the active group calls shall stop timer TNG3 (group call timer) for each group call, and the controlling MCPTT function hosting the temporary group call shall start timer TNG3 (group call timer) for the temporary group call.

NOTE 2: If the MCPTT server(s) hosting the independent active group calls are different to the MCPTT server that will host the temporary group call, then the MCPTT server(s) hosting the independent active group calls become non-controlling MCPTT function(s) of an MCPTT group, for the temporary group call.

When splitting a temporary group call into independent group calls, the controlling MCPTT function hosting the temporary group call shall stop timer TNG3 (group call timer) and the controlling MCPTT function(s) hosting the independent group calls shall start TNG3 (group call timer) for each group call.

When the last MCPTT client leaves the MCPTT session, the controlling MCPTT function shall stop timer TNG3 (group call timer).

On expiry of timer (group call timer), the controlling MCPTT function shall release the MCPTT session by following the procedures in subclause 6.3.3.1.5;

6.3.3.5.2 Interaction with the in-progress emergency group call timer (TNG2)

If the controlling MCPTT function starts timer TNG2 (in-progress emergency group call timer), it shall not start timer TNG3 (group call timer).

If timer TNG3 (group call timer) is running and the MCPTT group call is upgraded to an MCPTT emergency group call, then the controlling MCPTT function shall stop timer TNG3 (group call timer) and shall start timer TNG2 (in-progress emergency group call timer) with the value obtained from the <group-time-limit> element of the <emergency-call> element of the <on-network> element of the service configuration document as specified in 3GPP TS 24.484 [50].If timer TNG2 (in-progress emergency group call timer) is running and the MCPTT emergency group call is cancelled, then the controlling MCPTT function shall stop timer TNG2 (in-progress emergency group call timer) and shall start timer TNG3 (group call timer) with the value obtained from the <on-network-maximum-duration> element of the group document as specified in 3GPP TS 24.481 [31].

If timer TNG2 (in-progress emergency group call timer) is running and subsequently expires, then the controlling MCPTT function shall start timer TNG3 (group call timer) with the value obtained from the <on-network-maximum-duration> element of the group document as specified in 3GPP TS 24.481 [31].

NOTE: The above conditions for starting timer TNG2 (in-progress emergency group call timer) and timer TNG3 (group call timer) also apply in the case that these timers are re-started. For example: the case where the timer TNG3 was initially running, the MCPTT group call is upgraded to an MCPTT emergency group call and then the MCPTT emergency group call is cancelled.

6.3.3.6 Void

6.3.4 Non-controlling MCPTT function of an MCPTT group

6.3.4.1 Request initiated by the non-controlling MCPTT function of an MCPTT group

6.3.4.1.1 SDP offer generation

The SDP offer is generated based on the received SDP offer. The SDP offer generated by the non-controlling MCPTT function of an MCPTT group:

1) shall include only one SDP media-level section for MCPTT speech as contained in the received SDP offer; and

2) shall include an SDP media-level section for one media-floor control entity, if present in the received SDP offer.

When composing the SDP offer according to 3GPP TS 24.229 [4], the non-controlling MCPTT function of an MCPTT group:

1) shall replace the IP address and port number for the offered media stream in the received SDP offer with the IP address and port number of the non-controlling MCPTT function;

2) shall include all media-level attributes from the received SDP offer;

3) shall replace the IP address and port number for the offered media floor control entity, if any, in the received SDP offer with the IP address and port number of the non-controlling MCPTT function; and

4) shall include the offered media floor control entity 'fmtp' attributes as specified in 3GPP TS 24.380 [5] clause 14.

6.3.4.1.2 Sending an INVITE request towards the MCPTT client

This subclause is referenced from other procedures.

The non-controlling MCPTT function of an MCPTT group shall generate initial SIP INVITE requests according to 3GPP TS 24.229 [4].

For each SIP INVITE request, the non-controlling MCPTT function of an MCPTT group:

1) shall generate a new MCPTT session identity for the MCPTT session with the invited MCPTT client and include it in the Contact header field together with the g.3gpp.mcptt media feature tag, the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt", and the isfocus media feature tag 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 set the Request-URI to the public service identity of the terminating participating MCPTT function associated to the MCPTT ID of the MCPTT user to be invited;

NOTE 1: How the non-controlling MCPTT function finds the address of the terminating participating MCPTT 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.

6) shall copy the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP INVITE request to the outgoing SIP INVITE request;

7) shall update the application/vnd.3gpp.mcptt-info+xml MIME body with: a <mcptt-request-uri> element set to the MCPTT ID of the invited MCPTT user;

8) shall include the public service identity of the non-controlling MCPTT function in the P-Asserted-Identity header field;

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

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

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

12) void

13) shall include an unmodified Answer-Mode header field, if present in the incoming SIP INVITE request;and

14) shall include the warning text set to "148 MCPTT group is regrouped" in a Warning header field as specified in subclause 4.4.

NOTE 3: As long as the MCPTT group is regrouped the floor control messages in the media plane includes a grouped regrouped indication as specified in 3GPP TS 24.380 [5].

6.3.4.1.3 Sending a SIP INFO request

This subclause is referenced from other procedures.

The non-controlling MCPTT function shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [4] and IETF RFC 6086 [64].

The non-controlling MCPTT function:

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

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcptt-request-uri> set to the temporary MCPTT group ID and the <mcptt-calling-group-id> element with the constituent MCPTT group ID; and

3) shall include an application/vnd.3gpp.mcptt-floor-request+xml MIME body with the Content-Disposition header field set to "Info-Package". For each current speaker the application/vnd.3gpp.mcptt-floor-request+xml MIME body shall be populated as follows:

   a) the <floor-type> element set to "general" or "dual" as described in subclause F.5.3;

   b) the SSRC of the MCPTT client with the permission to send media in the <ssrc> element;

   c) the actual floor priority in the <floor-priority> element;

   d) the MCPTT ID of the MCPTT user with the permission to send media in the <user-id> element;

   e) the queueing capability in the <queueing-capability> element of the <track-info> element;

   f) the participant type in the <participant-type> in the <track-info> element;

   g) one or more <floor-participant-reference> elements in the <track-info> element in the same order as the would appear in the Track Info field as specified in 3GPP TS 24.380 [5] subclause 8.2.3.13; and

h) if available, additional information in the <floor-indicator> element.

6.3.4.1.4 Sending an INVITE request towards the controlling MCPTT function

This subclause is referenced from other procedures.

The non-controlling MCPTT function shall generate a SIP INVITE request according to rules and procedures of 3GPP TS 24.229 [4].

The non-controlling MCPTT function:

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

2) 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;

3) shall set the Request-URI to the public service identity of the controlling MCPTT function based on the <mcptt-request-uri> element received in the "SIP INVITE request for controlling MCPTT function of an MCPTT group";

NOTE 1: How the non-controlling MCPTT function finds the address of the controlling MCPTT 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.

4) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with:

   a) the <session-type> element set to "prearranged";

NOTE 3: The <session-type> element set to "prearranged" regardless of which type of group the constituent MCPTT group is.

   b) the <mcptt-request-uri> element set to the TGI retrieved from the <on-network-regrouped> element in the group document;

   c) the <mcptt-calling-user-id> element set to the constituent MCPTT group ID; and

   d the <required> element set to "true", if the group document retrieved from the group management server contains <on-network-required> group members as specified in 3GPP TS 24.481 [31];

5) shall include the public service identity of the non-controlling MCPTT function in the P-Asserted-Identity header field;

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

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

6.3.4.2 Requests terminated by the non-controlling MCPTT function of an MCPTT group

6.3.4.2.1 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [4], the non-controlling MCPTT function of an MCPTT group:

1) for the accepted media stream in the received SDP offer:

   a) shall replace the IP address and port number in the received SDP offer with the IP address and port number of the non-controlling MCPTT function; and

2) for the accepted media-floor control entity, if present in the received SDP offer:

   a) shall replace the IP address and port number in the received SDP offer with the IP address and port number of the non-controlling MCPTT function; and

   b) shall include 'fmtp' attributes as specified in 3GPP TS 24.380 [5] clause 14.

6.3.4.2.2 Sending a SIP response to the SIP INVITE request

6.3.4.2.2.1 Sending a SIP 183 (Session Progress) response

When sending a SIP 183 (Session Progress) the non-controlling MCPTT function of an MCPTT group:

1) shall generate a SIP 183 (Session Progress) response according to 3GPP TS 24.229 [4];

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

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

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

3) shall include the public service identity of the non-controlling MCPTT function in the P-Asserted-Identity header field; and

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

6.3.4.2.2.2 Sending a SIP 200 (OK) response

When sending a SIP 200 (OK) response, the non-controlling MCPTT function of an MCPTT group:

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 the public service identity of the non-controlling MCPTT function in the P-Asserted-Identity header field;

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

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

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

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

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

8) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcptt-called-party-id> element set to the constituent MCPTT group ID and the <floor-state> element set to the state of the floor.

6.3.4.3 Generating a SIP NOTIFY request

The non-controlling MCPTT function shall generate a SIP NOTIFY request according to 3GPP TS 24.229 [4] with the clarification in this subclause.

In the SIP NOTIFY request, the non-controlling MCPTT function:

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

2) shall include an Event header field set to the "conference" event package;

3) shall include an Expires header field set to 3600 seconds according to IETF RFC 4575 [30], as default value;

4) 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-Preferred-Service header field according to IETF RFC 6050 [9]; and

5) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with:

   a) the <mcptt-calling-group-id> set to the value of the constituent MCPTT group ID;

   b) if the target is a MCPTT user, the value of <mcptt-request-uri> element set to the MCPTT ID of the targeted MCPTT user; and

   c) if the target is the controlling MCPTT function the value of <mcptt-request-uri> element set to the temporary MCPTT group ID.

In the SIP NOTIFY request, the non-controlling MCPTT function shall include application/conference-info+xml MIME body according to IETF RFC 4575 [30] as specified in subclause 6.3.3.4 with the following exceptions:

1) the non-controlling MCPTT function shall not regard the controlling MCPTT function as a participant and not include the controlling MCPTT function in a <user> element; and

NOTE: The controlling MCPTT function initiated the temporary group call and will appear as a participant in the group session.

2) the non-controlling MCPTT function shall include stored conference status information received in SIP NOTIFY requests from the non-controlling MCPTT function in subclause 10.1.3.5.3 and status information about own participants.

6.3.4.4 Void

6.3.5 Retrieving and processing a group document

6.3.5.1 General

This subclause describes how an MCPTT server accesses a group document from a group management server. The MCPTT server which accesses a group document performs the role of a controlling MCPTT function or performs the role of a non-controlling MCPTT function of an MCPTT group when accessing a group document. In such cases, for a group call:

- the controlling MCPTT function and group management server are both located in the primary MCPTT system;

- the controlling MCPTT function and group management server are both located in a partner MCPTT system;

- the controlling MCPTT function is located in the primary MCPTT system and accesses a group management server in the primary MCPTT system and a non-controlling MCPTT function of an MCPTT group is located in a partner MCPTT system and accesses a group management server in the partner MCPTT system; or

- the controlling MCPTT function and non-controlling MCPTT function(s) of an MCPTT group are located in the primary MCPTT system and access group management servers in the primary MCPTT system.

When the MCPTT server receives a SIP INVITE request that requires it to access a group document, it uses an MCPTT group ID or a temporary MCPTT group identity (TGI) which was created by the group regrouping operation as specified in 3GPP TS 24.481 [31].

The MCPTT server can cache the group document associated with an MCPTT group or temporary group, and can subscribe to be notified of changes to the group document associated with an MCPTT group or temporary group as specified in 3GPP TS 24.481 [31].

NOTE 1: During the group regrouping operation as specified in 3GPP TS 24.481 [31], the controlling MCPTT function is notified of the constituent MCPTT group identities associated with the TGI.

If the group data associated with an MCPTT group ID or TGI cached in the MCPTT server is removed, the MCPTT server re-subscribes for changes in the group information associated with the MCPTT group ID or TGI.

NOTE 2: Re-subscription can occur prior to the receipt of an SIP INVITE request containing an MCPTT group ID or TGI of a group document which is no longer cached on the MCPTT server.

6.3.5.2 Rules for retrieving Group Document(s)

NOTE 1: In this subclause, "MCPTT server" can refer to either the controlling MCPTT function of an MCPTT group or the non-controlling MCPTT function of an MCPTT group.

Upon receipt of a SIP INVITE request:

1) if the MCPTT server is not yet subscribed to the group document for the group identity in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request, the MCPTT server shall subscribe to the "xcap-diff" event-package for the group document of this group identity as specified in 3GPP TS 24.481 [31];

NOTE 2: The group identity in the <mcptt-request-uri> element is either an MCPTT group ID or a temporary MCPTT group identity (TGI).

NOTE 3: As a group document can potentially have a large content, the controlling MCPTT function of an MCPTT group can subscribe to the group document indicating support of content-indirection as defined in IETF RFC 4483 [32], by following the procedures in 3GPP TS 24.481 [31].

2) upon receipt of a SIP 404 (Not Found) response as a result of attempting to subscribe to the "xcap-diff" event-package for the group document of the group identity in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request as specified in 3GPP TS 24.481 [31], the MCPTT server shall send the SIP 404 (Not Found) response with the warning text set to "113 group document does not exist" in a Warning header field as specified in subclause 4.4. Otherwise, continue with the rest of the steps;

3) upon receipt of any other SIP 4xx, SIP 5xx or SIP 6xx response as a result of attempting to subscribe to the "xcap-diff" event-package for the group document of the group identity in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request as specified in 3GPP TS 24.481 [31], the MCPTT server shall send the SIP final response with the warning text set to "114 unable to retrieve group document" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

4) upon receipt of a notification from the group management server containing the group document for the group identity in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info MIME body of the SIP INVITE request, or if the group document is already cached:

   a) if the MCPTT server is a non-controlling function of an MCPTT group, then the MCPTT server shall exit this subclause; and

   b) if the MCPTT server is a controlling function of an MCPTT group, then the MCPTT server shall determine if the group document is for a TGI or an MCPTT group ID as follows:

      i) if the group document includes an <on-network-temporary> element, then the group document is associated with a TGI;

      ii) if the group document does not include an <on-network-temporary> element or an <on-network-regrouped> element, then the group document is associated with an MCPTT ID that has not been regrouped; and

      iii) if the group document does not include an <on-network-temporary> element but includes an <on-network-regrouped> element, then the group document is associated with an MCPTT ID that has been regrouped;

5) if the SIP INVITE request is a "SIP INVITE request for controlling function of an MCPTT group" and the group identity in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP-INVITE request is an MCPTT group ID that has not been re-grouped, the MCPTT server shall access the following elements from the group document as specified in 3GPP TS 24.481 [31]:

a) if the <on-network-disabled> element is present in the group document, shall send a SIP 403 (Forbidden) response with the warning text set to "115 group is disabled" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

b) if the <list> element of the <list-service> element does not contain an entry matching the MCPTT ID of the user in the SIP INVITE request, shall send a SIP 403 (Forbidden) response with the warning text set to "116 user is not part of the MCPTT group" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

c) if the <on-network-invite-members> element is set to "true" and if the SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <session-type> element containing a value not set to "prearranged", shall return a SIP 404 (Not Found) response with the warning text set to "117 the group identity indicated in the request is a prearranged group" as specified in subclause 4.4 "Warning header field" and shall not continue with the rest of the steps; and

d) if the <on-network-invite-members> element is set to "false" and if the SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <session-type> element containing a value not set to "chat" shall return a SIP 404 (Not Found) response with the warning text set to "118 the group identity indicated in the request is a chat group" as specified in subclause 4.4 "Warning header field" and shall not continue with the rest of the steps;

6) if the SIP INVITE request is a "SIP INVITE request for controlling function of an MCPTT group" and the group document for the group identity in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info MIME body of the SIP INVITE request is associated with an MCPTT group ID that has been regrouped, the MCPTT server:

a) shall obtain the TGI associated with the regrouped group, by accessing the "temporary-MCPTT-group-ID" attribute of the <regrouped> element of the group document associated with the MCPTT ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info MIME body of the SIP INVITE request;

b) if not hosting the TGI, shall:

i) stop processing the SIP INVITE request; and

ii) return a SIP 302 (Moved Temporarily) response with:

A) a Contact header field set to the PSI of the MCPTT server hosting the TGI; and

B) an application/vnd.3gpp.mcptt-info MIME body with a <mcptt-request-uri> element set to the TGI; and

c) if hosting the TGI, and the call to the temporary group is in progress, shall:

i) associate the MCPTT ID of the calling user with the temporary group call;

ii) interact with the media plane as specified in 3GPP TS 24.380 [5]; and

iii) exit this subclause;

d) if hosting the TGI and the call to the temporary group is not in progress, shall subscribe to the "xcap-diff" event-package for the group document of the TGI as specified in 3GPP TS 24.481 [31], if not already subscribed;

e) upon receipt of a SIP 404 (Not Found) response as a result of attempting to subscribing to the "xcap-diff" event-package for the group document(s) for the MCPTT group ID(s) associated to the TGI as specified in 3GPP TS 24.481 [31], shall send the SIP 404 (Not Found) response with the warning text set to "113 group document does not exist" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

f) upon receipt of any other SIP 4xx, SIP 5xx or SIP 6xx response as a result of attempting to subscribe to the "xcap-diff" event-package for the group document(s) for the MCPTT group ID(s) associated to the TGI as specified in 3GPP TS 24.481 [31], shall send the SIP final response with the warning text set to "114 unable to retrieve group document" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

g) upon receipt of a notification containing the group document for the TGI, or if the group document is already cached, shall obtain the MCPTT IDs of the constituent groups by accessing the <constituent-MCPTT-group-ID> element(s) of the group document for the TGI; and

h) if:

i) the <associated-group-id> element with an MCPTT ID is included in the application/vnd.3gpp.mcptt-info MIME body;

ii) the MCPTT ID is present in one of the instances of the <constituent-MCPTT-group-ID> element in the group document; and

iii) the group is not homed by the MCPTT server;

shall exit this procedure and authorize the MCPTT user at a non-controlling MCPTT function of a MCPTT group;

NOTE 4: The non-controlling function of an MCPTT group can be located in the primary MCPTT system or a partner MCPTT system.

7) for the MCPTT ID of each constituent group, shall follow the actions below in step 8); and

8) if the SIP INVITE request is a "SIP INVITE request for controlling function of an MCPTT group" and the group document for the group identity in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info MIME body of the SIP INVITE request retrieved is associated with a TGI and if:

a) the application/vnd.3gpp.mcptt-info+xml includes an <associated-group-id> element, determine if the constituent MCPTT group identified by the <associated-group-id> element is homed at the MCPTT server and if that is the case:

i) shall subscribe to the "xcap-diff" event-package for the group document for the constituent MCPTT group ID as specified in 3GPP TS 24.481 [31], if not already subscribed;

ii) upon receipt of a SIP 404 (Not Found) response as a result of attempting to subscribing to the "xcap-diff" event-package for the group document for the MCPTT group ID associated to the TGI as specified in 3GPP TS 24.481 [31], shall send the SIP 404 (Not Found) response with the warning text set to "113 group document does not exist" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps; and

iii) upon receipt of any other SIP 4xx, SIP 5xx or SIP 6xx response as a result of attempting to subscribe to the "xcap-diff" event-package for the group document for the MCPTT group ID associated to the TGI as specified in 3GPP TS 24.481 [31], shall send the SIP final response with the warning text set to "114 unable to retrieve group document" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps; and

b) the application/vnd.3gpp.mcptt-info+xml does not include an <associated-group-id> element, for each MCPTT ID contained in each instance of the <constituent-MCPTT-group-ID> element of the group document for the TGI:

i) shall determine if the group identity is homed on the controlling MCPTT function of an MCPTT group or homed on a non-controlling MCPTT function of an MCPTT group;

NOTE 5: The non-controlling function of an MCPTT group can be located in the primary MCPTT system or a partner MCPTT system.

ii) for each constituent MCPTT group ID that is homed on the controlling MCPTT function of an MCPTT group shall subscribe to the "xcap-diff" event-package for the group document for the constituent MCPTT group ID as specified in 3GPP TS 24.481 [31], if not already subscribed;

NOTE 6: As soon as an error occurs when subscribing for a group document of a constituent MCPTT group ID, the controlling MCPTT function of an MCPTT group stops subscribing to any further group documents of constituent MCPTT group IDs.

iii) upon receipt of a SIP 404 (Not Found) response as a result of attempting to subscribing to the "xcap-diff" event-package for the group document(s) for the MCPTT group ID(s) associated to the TGI as specified in 3GPP TS 24.481 [31], shall send the SIP 404 (Not Found) response with the warning text set to "113

group document does not exist" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

iv) upon receipt of any other SIP 4xx, SIP 5xx or SIP 6xx response as a result of attempting to subscribe to the "xcap-diff" event-package for the group document(s) for the MCPTT group ID(s) associated to the TGI as specified in 3GPP TS 24.481 [31], shall send the SIP final response with the warning text set to "114 unable to retrieve group document" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps; and

c) when all group document(s) for all constituent groups homed at the MCPTT server have been retrieved and if the MCPTT ID of the user identified in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body:

i) is a member of one the retrieved constituent MCPTT groups, received, shall exit this procedure; and

ii) is not a member of any of the retrieved constituent group documents, shall determine that the MCPTT ID of the MCPTT user needs to be authorised by a non-controlling MCPTT function of an MCPTT group and exit this procedure.

6.3.5.3 Rules for joining a group session

The following conditions shall be met for the controlling MCPTT function to allow an MCPTT user to join an existing group session:

1) an <entry> element exists in the <list> element of the group document for the MCPTT user;

2) a <rule> exists in the group document with:

a) the <is-list-member> element of the <conditions> element present and with the <join-handling> element of the corresponding <actions> element set to "true"; or

b) the <identity> element of the <conditions> element containing an entry matching the MCPTT ID in the SIP INVITE request, with the <join-handling> element of the <actions> element set to "true"; and

3) if the <supported-services> element is present, it contains:

a) a <service> element containing an "enabler" attribute which is set to the MCPTT ICSI; and

b) if a <group-media> element is present, an entry set to "MCPTT speech".

If all of the above conditions are not met, then the MCPTT user shall not be authorised to join the group session.

6.3.5.4 Rules for initiating a prearranged group session

The following conditions shall be met for a controlling MCPTT function or non-controlling MCPTT function of an MCPTT group to initiate a group session for the requesting MCPTT user:

1) if the <on-network-regrouped> element in the <list-service> element is present in the group document and if the MCPTT ID indicated in the incoming INVITE request is the same as the MCPTT group ID in the "temporary-MCPTT-group-ID" attribute of the <on-network-regrouped> element; or

2) if the <on-network-regrouped> element in the <list-service> element of the MCPTT group document is not present in the group document;

and:

1) an <entry> element exists in the <list> element of the group document for the MCPTT user;

2) a <rule> exists in the group document with:

a) the <is-list-member> element of the <conditions> element present and with the <allow-initiate-conference> element of the corresponding <actions> element set to "true"; or

b) the <identity> element of the <conditions> element containing an entry matching the MCPTT ID in the SIP INVITE request, with the <allow-initiate-conference> element of the <actions> element is set to "true"; and

3) if the <supported-services> element is present, it contains:

   a) a <service> element containing an "enabler" attribute which is set to the MCPTT ICSI; and

   b) if a <group-media> element is present, an entry set to "MCPTT speech".

then the MCPTT user shall not be authorised to initiate the group session.

6.3.5.5 Determining the group members to invite

The MCPTT server shall only invite affiliated group members to a group session. The MCPTT server determines the affiliated members from the entries contained in the <list> element of the group document by following the procedures specified in subclause 6.3.6.

NOTE 1: The term "affiliated group members" used above also includes those members that are implicitly affiliated by the controlling MCPTT function.

If the number of members of the MCPTT group exceeds the value contained in the <on-network-max-participant-count> element the MCPTT server shall invite only <on-network-max-participant-count> members from the list, but shall prioritise inviting those group members to the group session that have an <entry> element in the <list> element with a <on-network-required> element present.

NOTE 2: The <on-network-max-participant-count> element indicates the maximum number of participants allowed in the group session. The <on-network-required> element is used to determine which group members need to acknowledge the group call before audio transmission can proceed.

NOTE 3: Other requirements for how the controlling MCPTT function selects which of the <on-network-max-participant-count> members to invite is outside the scope of this specification.

NOTE 4: It is assumed that validation checks are performed at the group management server to ensure that the <on-network-max-participant-count> cannot be less than the number of <on-network-required> users.

6.3.6 Affiliation check

The MCPTT server checks if an MCPTT user is affiliated to an MCPTT group at an MCPTT client by following the procedures specified below:

1. the MCPTT server shall find the applicable MCPTT group information entry as an MCPTT group information entry of the list of MCPTT group information entries described in subclause 9.2.2.3.2, such that the MCPTT group ID of the MCPTT group information entry is equal to the MCPTT group identity of the MCPTT group. If the applicable MCPTT group information entry cannot be found, then the MCPTT server shall determine that the MCPTT user is not affiliated to the MCPTT group at the MCPTT client and the MCPTT server shall not continue with rest of the steps;

2. the MCPTT server shall find the applicable MCPTT user information entry as an MCPTT user information entry of the list of MCPTT user information entries of the applicable MCPTT group information entry, such that the MCPTT ID of the MCPTT user information entry is equal to the MCPTT ID of the MCPTT user. If the applicable MCPTT user information entry cannot be found, then the MCPTT server shall determine that the MCPTT user is not affiliated to the MCPTT group at the MCPTT client and the MCPTT server shall not continue with rest of the steps;

3. if the MCPTT client ID of the MCPTT client cannot be found in the list of MCPTT client information entries of the applicable MCPTT user information entry, then the MCPTT server shall determine that the MCPTT user is not affiliated to the MCPTT group at the MCPTT client and the MCPTT server shall not continue with rest of the steps;

NOTE: the MCPTT client ID of the originating MCPTT client can be found in the <mcptt-client-id> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body of a SIP INVITE request, SIP REFER request or SIP MESSAGE request originated by the MCPTT client.

4. if the expiration time of the applicable MCPTT user information entry has been reached, then the MCPTT server shall determine that the MCPTT user is not affiliated to the MCPTT group at the MCPTT client and the MCPTT server shall not continue with rest of the steps; and

5. the MCPTT server shall determine that the MCPTT user is affiliated to the MCPTT group at the MCPTT client.

6.3.7 Error handling

6.3.7.1 Public service identity does not exist

Upon receiving a request that includes the Request-URI set to a public service identity that is not allocated in the participating or the controlling MCPTT function, the participating or the controlling MCPTT function shall return a SIP 404 (Not Found) response.

6.3.8 Session release policy

6.3.8.1 Session release policy for group call

If:

1) the call is a pre-arranged group call and if the controlling MCPTT function receives an indication from the media plane that the T4 (Inactivity) timer specified in 3GPP TS 24.380 [5] expired;

2) there are only one or no participants in the MCPTT session;

3) if the call is a pre-arranged group call and if it is according to local policy, the initiator of the group call leaves the MCPTT session;

4) the minimum number of affiliated MCPTT group members is not present; or

5) timer TNG3 (group call timer) expires;

the controlling MCPTT function shall release the MCPTT session for the group call.

6.3.8.2 Session release policy for private call

If:

1) the controlling MCPTT function receives an indication from the media plane that the T4 (Inactivity) timer specified in 3GPP TS 24.380 [5] expired;

2) the MCPTT session has lasted longer than the maximum of duration of private call; or

3) there are only one or no participants in the MCPTT session;

the controlling MCPTT function shall release the MCPTT session for a private call.

6.4 Implicit floor request

An initial SIP INVITE request fulfilling the following criteria shall be regarded by the MCPTT server as an implicit floor request by the originating MCPTT client when the MCPTT client:

1) initiates an MCPTT speech session or initiates a pre-established session that is not used for a remotely initiated MCPTT ambient listening call; and

2) includes the "mc_implicit_request" 'fmtp' attribute in the associated UDP stream for the floor control in the SDP offer/answer as specified in 3GPP TS 24.380 [5] clause 12.

An initial SIP INVITE request fulfilling the following criteria shall be regarded by the MCPTT server as an implicit request to grant the floor to the terminating MCPTT client when the originating MCPTT client:

1) initiates a remotely initiated MCPTT ambient listening call; and

2) includes the "mc_implicit_request" 'fmtp' attribute in the associated UDP stream for the floor control in the SDP offer/answer as specified in 3GPP TS 24.380 [5] clause 12.

A SIP re-INVITE request fulfilling the following criteria shall be regarded by the MCPTT server as an implicit floor request when the MCPTT client:

1) performs an upgrade of:

   a) an MCPTT group call to an emergency MCPTT group call;

   b) an MCPTT private call to an emergency MCPTT private call; or

   c) an MCPTT group call to an imminent peril MCPTT group call; and

2) includes the "mc_implicit_request" 'fmtp' attribute in the associated UDP stream for the floor control in the SDP offer/answer as specified in 3GPP TS 24.380 [5] clause 12.

In all other cases the SIP (re-)INVITE request shall be regarded as received without an implicit floor request.

When using a pre-established session the MCPTT server shall regard the SIP REFER request as an implicit floor request:

1) if the pre-established session was established with an implicit floor request and if an SDP offer is not included in a "body" parameter in the headers portion of the SIP URI in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field;

2) if the pre-established session was established with an implicit floor request, an SDP offer is included in a "body" parameter in the headers portion of the SIP URI in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field, and this SDP includes the "mc_implicit_request" media level attribute in the associated UDP stream for the floor control in the SDP offer; or

3) if the pre-established session was established without an implicit floor request and the SDP offer in a "body" parameter in the headers portion of the SIP URI in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field includes the "mc_implicit_request" media level attribute in the associated UDP stream for the floor control in the SDP offer.

In all other cases the SIP REFER request shall be regarded as received without an implicit floor request.

When using a pre-established session the MCPTT server shall regard the SIP REFER request as an implicit request to grant the floor to the terminating MCPTT client:

1) if the pre-established session was established with an SDP offer included in a "body" parameter in the headers portion of the SIP URI in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field, and this SDP includes the "mc_implicit_request" media level attribute in the associated UDP stream for the floor control in the SDP offer; and

2) the pre-established session is being used for a remotely initiated ambient listening call.

In all other cases the SIP REFER request shall be regarded as received without an implicit request to grant the floor to the terminating MCPTT client.

6.5 Handling of MIME bodies in a SIP message

The MCPTT client and the MCPTT server shall support several MIME bodies in SIP request and SIP responses.

When the MCPTT client or the MCPTT server sends a SIP message and the SIP message contains more than one MIME body, the MCPTT client or the MCPTT server:

1) shall, as specified in IETF RFC 2046 [21], include one Content-Type header field with the value set to multipart/mixed and with a boundary delimiter parameter set to any chosen value;

2) for each MIME body:

   a) shall insert the boundary delimiter;

   b) shall insert the Content-Type header field with the MIME type of the MIME body; and

c) shall insert the content of the MIME body;

3) shall insert a final boundary delimiter; and

4) if an SDP offer or an SDP answer is one of the MIME bodies, shall insert the application/sdp MIME body as the first MIME body.

NOTE: The reason for inserting the application/sdp MIME body as the first body is that if a functional entity in the underlying SIP core does not understand multiple MIME bodies, the functional entity will ignore all MIME bodies with the exception of the first MIME body. The order of multiple MCPTT application MIME bodies in a SIP message is irrelevant.

When the MCPTT client or the MCPTT server sends a SIP message and the SIP message contains only one MIME body, the MCPTT client or the MCPTT server:

1) shall include a Content-Type header field set to the MIME type of the MIME body; and

2) shall insert the content of the MIME body.

6.6 Confidentiality and Integrity Protection

6.6.1 General

6.6.1.1 Applicability and exclusions

The procedures in subclauses 6.6 apply in general to all procedures described in clause 9, clause 10, clause 11 and clause 12 with the exception that the confidentiality and integrity protection procedures for the registration and service authorisation procedures are described in clause 7.

6.6.1.2 Performing XML content encryption

Whenever the MCPTT UE includes XML elements or attributes pertaining to the data specified in subclause 4.8 in SIP requests or SIP responses, the MCPTT UE shall perform the procedures in subclause 6.6.2.3.1.

Whenever the MCPTT server includes XML elements or attributes pertaining to the data specified in subclause 4.8 in SIP requests or SIP responses, the MCPTT server shall perform the procedures in subclause 6.6.2.3.2, with the exception that when the MCPTT server receives a SIP request with XML elements or attributes in an MIME body that need to be copied from the incoming SIP request to an outgoing SIP request without modification, the MCPTT server shall perform the procedures specified in subclause 6.6.2.5.

NOTE: The procedures in subclause 6.6.2.3.1 and subclause 6.6.2.3.2 first determine (by referring to configuration) if confidentiality protection is enabled and then call the necessary procedures to encrypt the contents of the XML elements if confidentiality protection is enabled.

6.6.1.3 Performing integrity protection on an XML body

The functional entity shall perform the procedures in the subclause just prior to sending a SIP request or SIP response.

1) The MCPTT UE shall perform the procedures in subclause 6.6.3.3.1; and

2) The MCPTT server shall perform the procedures in subclause 6.6.3.3.2.

NOTE: The procedures in subclause 6.6.3.3.1 and subclause 6.6.3.3.2 first determine if integrity protection of XML MIME bodies is required and then calls the necessary procedures to integrity protect each XML MIME body if integrity protection is required. Each XML MIME body has its own signature.

6.6.1.4 Verifying integrity of an XML body and decrypting XML elements

Whenever the functional entity (i.e. MCPTT UE or MCPTT server) receives a SIP request or a SIP response, the functional entity shall perform the following procedures before performing any other procedures.

1) The functional entity shall determine if integrity protection has been applied to an XML MIME body by following the procedures in subclause 6.6.3.4.1 and if integrity protection has been applied:

   a) shall use the keying information described in subclause 6.6.3.2 and the procedures described in subclause 6.6.3.4.2 to verify the integrity of the XML MIME body; and

   b) if the integrity protection checks fail shall not perform any further procedures in this clause;

2) The functional entity shall determine whether confidentiality protection has been applied to XML elements in XML MIME bodies in a SIP request or SIP response, pertaining to the data specified in subclause 4.8, by following the procedures in subclause 6.6.2.4.1, and if confidentiality protection has been applied:

   a) shall use the keying information described in subclause 6.6.2.2 along with the procedures described in subclause 6.6.2.4.2 to decrypt the received values; and

   b) if any decryption procedures fail, shall not perform any further procedures in this clause.

6.6.2 Confidentiality Protection

6.6.2.1 General

In general, confidentiality protection is applied to specific XML elements and attributes in XML MIME bodies in SIP requests and responses as specified in subclause 4.8. However in the case of SIP REFER requests used for pre-established sessions, confidentiality protection is required for:

the targeted MCPTT ID or MCPTT Group ID, placed in a "uri" attribute of an <entry> element of an application/resource-lists+xml MIME body that is pointed to by a "cid" URL located in the Refer-To header field of the SIP REFER request; and

- sensitive XML data included in MIME bodies which are placed in the hname "body" URI header field of the URI included in the "uri" attribute of the <entry> element of the application/resource-lists+xml MIME body.

Configuration for applying confidentiality protection is not selective to a specific XML element or attribute of the data described in subclause 4.8. If configuration for confidentiality protection is turned on, then all XML elements and attributes described in subclause 4.8 are confidentiality protected. If configuration for confidentiality protection is turned off, then no XML content in SIP requests and SIP responses are confidentiality protected.

6.6.2.2 Keys used in confidentiality protection procedures

Confidentiality protection uses an XPK to encrypt the data which (depending on who is the sender and who is the receiver of the encrypted information) can be a CSK or an SPK as specified in subclause 4.8. An XPK-ID (CSK-ID/SPK-ID) is used to key the XPK (CSK/SPK). It is assumed that before the procedures in this subclause are called, the CSK/CSK-ID and/or SPK/SPK-ID are available on the sender and recipient of the encrypted content as described in subclause 4.8.

The procedures in subclause 6.6.2.3 and subclause 6.6.2.4 are used with a XPK equal to the CSK and a XPK-ID equal to the CSK-ID in the following circumstances as described in 3GPP TS 33.180 [78]:

1) MCPTT client sends confidentiality protected content to an MCPTT server; and

2) MCPTT server sends confidentiality protected content to an MCPTT client.

The procedure in subclause 6.6.2.3 and subclause 6.6.2.4 are used with a XPK equal to the SPK and a XPK-ID equal to the SPK-ID in the following circumstances as described in 3GPP TS 33.180 [78]:

1) MCPTT server sends confidentiality protected content to an MCPTT server in the same domain; and

2) MCPTT server sends confidentiality protected content to an MCPTT server in another domain.

6.6.2.3 Procedures for sending confidentiality protected content

6.6.2.3.1 MCPTT client

If the <confidentiality-protection> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "true" or no <confidentiality-protection> element is present in the Service Configuration document, then sending confidentiality protected content from the MCPTT client to the MCPTT server is enabled, and the MCPTT client:

1) shall use the appropriate keying information specified in subclause 6.6.2.2;

2) shall perform the procedures in subclause 6.6.2.3.3 to confidentiality protect XML elements containing the content described in subclause 4.8; and

3) shall perform the procedures in subclause 6.6.2.3.4 to confidentiality protect URIs in XML attributes for URIs described in subclause 4.8.

If the <confidentiality-protection> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "false", then sending confidentiality protected content from the MCPTT client to the MCPTT server is disabled, and content is included in XML elements and attributes without encryption.

6.6.2.3.2 MCPTT server

If the <confidentiality-protection> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "true" or no <confidentiality-protection> element is present in the Service Configuration document, then sending confidentiality protected content from the MCPTT server to the MCPTT client is enabled. If the <allow-signalling-protection> element of the <protection-between-mcptt-servers> element is set to "true" in the Service Configuration document as specified in 3GPP TS 24.484 [50] or no <allow-signalling-protection> element is present in the Service Configuration document, then sending confidentiality protected content between MCPTT servers is enabled.

When sending confidentiality protected content, the MCPTT server:

1) shall use the appropriate keying information specified in subclause 6.6.2.2;

2) shall perform the procedures in subclause 6.6.2.3.3 to confidentiality protect XML elements containing the content described in subclause 4.8, and

3) shall perform the procedures in subclause 6.6.2.3.4 to confidentiality protect URIs in XML attributes for URIs described in subclause 4.8.

If the <confidentiality-protection> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "false", then sending confidentiality protected content from the MCPTT server to the MCPTT client is disabled, and then content is included in XML elements and attributes without encryption.

If the <allow-signalling-protection> element of the <protection-between-mcptt-servers> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "false", then sending confidentiality protected content between MCPTT servers is disabled, and content is included in XML elements and attributes without encryption.

6.6.2.3.3 Content Encryption in XML elements

The following procedures shall be performed by an MCPTT client or an MCPTT server:

1) perform encryption as specified in W3C: "XML Encryption Syntax and Processing Version 1.1", https://www.w3.org/TR/xmlenc-core1/ [60] subclause 4.3, using the "AES-128-GCM algorithm HMAC" as the encryption algorithm and the XPK as the key; and

2) follow the semantic for the element of the MIME body as described in Annex F of the present document, to include the encrypted content in the MIME body ensuring that the necessary XML elements required for confidentiality protection are included as specified in 3GPP TS 33.180 [78].

6.6.2.3.4 Attribute URI Encryption

The following procedures shall be performed by an MCPTT client or an MCPTT server:

1) perform encryption as specified in [aes-gcm], using the "AES-128-GCM algorithm HMAC" as the encryption algorithm and the XPK as the key, with a 96 bit randomly selected IV; and

2) replace the URI to be protected in the attribute by a URI constructed as follows:

   a) the URI schema is "sip:";

   b) the first part of the userinfo part is the base64 encoded result of the encryption of the original attribute value;

   c) the string ";iv=" is appended to the result of step b);

   d) the base64 encoding of the IV (section 5 of IETF RFC 4648 [71]) is appended to the result of step c);

   e) the string ";key-id=" is appended to the result of step d);

   f) the base64 encoding of the XPK-ID according to 3GPP 33.180 [78] is appended to the result of step e);

   g) the string ";alg=128-aes-gcm" is appended to the result of step f); and

   h) the string "@" followed by the domain name for MCPTT confidentiality protection as specified in 3GPP TS 23.203is appended to the result of step g).

6.6.2.4 Procedures for receiving confidentiality protected content

6.6.2.4.1 Determination of confidentiality protected content

The following procedure is used by the MCPTT client or MCPTT server to determine if an XML element is confidentiality protected.

1) if an XML element contains the <EncryptedData> XML element, then the content of the XML element is confidentiality protected; and

2) if an XML element does not contain the <EncryptedData> XML element, then the content of the XML element is.not confidentiality protected.

The following procedure is used by the MCPTT client or MCPTT server to determine if a URI in the XML attribute is confidentiality protected.

1) if an XML attribute is a URI with the domain name for MCPTT confidentiality protection as specified in the 3GPP TS 23.003 [40], then the URI is confidentiality protected; and

2) if an XML attribute is a URI without the domain name for MCPTT confidentiality protection as specified in the 3GPP TS 23.003 [40], then the URI is not confidentiality protected.

6.6.2.4.2 Decrypting confidentiality protected content in XML elements

The following procedure shall be performed by an MCPTT client or an MCPTT server to decrypt an individual XML element that has a type of "encrypted" within an XML MIME body:

1) if the <EncryptedData> XML element or any of its sub-elements as described in 3GPP TS 33.180 [78] are not present in the MIME body then send a SIP 403 (Forbidden) response with the warning text set to "140 unable to decrypt XML content" in a Warning header field as specified in subclause 4.4, and exit this procedure. Otherwise continue with the rest of the steps;

2) perform decryption on the <EncryptedData> element as specified in W3C: "XML Encryption Syntax and Processing Version 1.1", https://www.w3.org/TR/xmlenc-core1/ [60] subclause 4.4 to decrypt the contents of the <CipherValue> element contained within the <CipherData> element;

3) if the decryption procedure fails, then send a SIP 403 (Forbidden) response with the warning text set to "140 unable to decrypt XML content" in a Warning header field as specified in subclause 4.4. Otherwise continue with the rest of the steps; and

4) return success of this procedure together with the decrypted XML element.

6.6.2.4.3 Decrypting confidentiality protected URIs in XML attributes

The following procedure shall be performed by an MCPTT client or an MCPTT server to decrypt a URI in an attribute in a XML document:

1) the value between ";iv=" and the next ";" provides the base64 encoded value of the 96 bit IV and the value between ";=key-id" and the next ";" defines the key which has been used for encryption, i.e. "CSK" or "SPK"; and

2) the original URI is obtained by decrypting the base64 encoded string between the "sip:" URI prefix and the next ";" using the "AES-128-GCM algorithm HMAC" as the decryption algorithm with IV and key as determined in step 1). This value replaces the encrypted URI as the value of the XML attribute.

6.6.2.5 MCPTT server copying received XML content

The following procedure is executed when an MCPTT server receives a SIP request containing XML MIME bodies, where the content needs to be copied from the incoming SIP request to the outgoing SIP request.

The MCPTT server:

1) shall copy the XML elements from the XML MIME body of the incoming SIP request that do not contain a <EncryptedData> XML element, to the same XML body in the outgoing SIP request;

2) for each encrypted XML element in the XML MIME body of the incoming SIP request as determined by subclause 6.6.2.4.1:

   a) shall use the keying information described in subclause 6.6.2.2 to decrypt the content within the XML element by following the procedures specified in subclause 6.6.2.4.2, and shall continue with the steps below if the encrypted XML element was successfully decrypted;

   b) if confidentiality protection is enabled as specified in subclause 6.6.2.3.2, then for each decrypted XML element:

      i) shall re-encrypt the content within the XML element using the keying information described in subclause 6.6.2.2 and by following the procedures specified in subclause 6.6.2.3.3; and

      ii) shall include the re-encrypted content into the same XML MIME body of the outgoing SIP request; and

   c) if confidentiality protection is disabled as specified in subclause 6.6.2.3.2, shall include the decrypted content in the same XML MIME body of the outgoing SIP request.

3) for each encrypted XML URI attribute in the XML MIME body of the incoming SIP request as determined by subclause 6.6.2.4.1:

   a) shall use the keying information described in subclause 6.6.2.2 to decrypt the URI value of the XML attribute by following the procedures specified in subclause 6.6.2.4.3, and shall continue with the steps below if the encrypted XML attribute value was successfully decrypted;

   b) if confidentiality protection is enabled as specified in subclause 6.6.2.3.2, then for each decrypted XML element:

      i) shall re-encrypt the URI value of the XML attribute using the keying information described in subclause 6.6.2.2 and by following the procedures specified in subclause 6.6.2.3.4; and

      ii) shall include the re-encrypted attribute value into the same XML MIME body of the outgoing SIP request; and

   c) if confidentiality protection is disabled as specified in subclause 6.6.2.3.2, shall include the decrypted value in the same XML MIME body of the outgoing SIP request.

6.6.3 Integrity Protection of XML documents

6.6.3.1 General

Integrity protection can be applied to a whole XML MIME body. When integrity protection is enabled, all XML MIME bodies transported in SIP requests and responses are integrity protected. The following XML MIME bodies used in the present specification in SIP signalling can be integrity protected:

- application/vnd.3gpp.mcptt-info+xml;
- application/poc-settings+xml;
- application/resources-list+xml;
- application/vnd.3gpp.mcptt-mbms-usage-info+xml;
- application/vnd.3gpp.mcptt-location-info+xml;
- application/vnd.3gpp.mcptt-affiliation-command+xml;
- application/vnd.3gpp.mcptt-floor-request+xml; and
- application/conference-info+xml.

If integrity protection is enabled, and one or more of the XML MIME bodies complying to the types listed above are included in a SIP request or SIP response, then a MIME body of type application/vnd.3gpp.mcptt-signed+xml is included in the SIP request or SIP response containing one or more signatures pointing to those XML MIME bodies as illustrated in Figure 6.6.3.3-1.

In order to integrity protect the XML MIME bodies listed above in this subclause in SIP requests and SIP responses, the MCPTT client and MCPTT server shall for each MIME body, include the Content-ID header field as specified in IETF RFC 2045 [68] containing a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62].

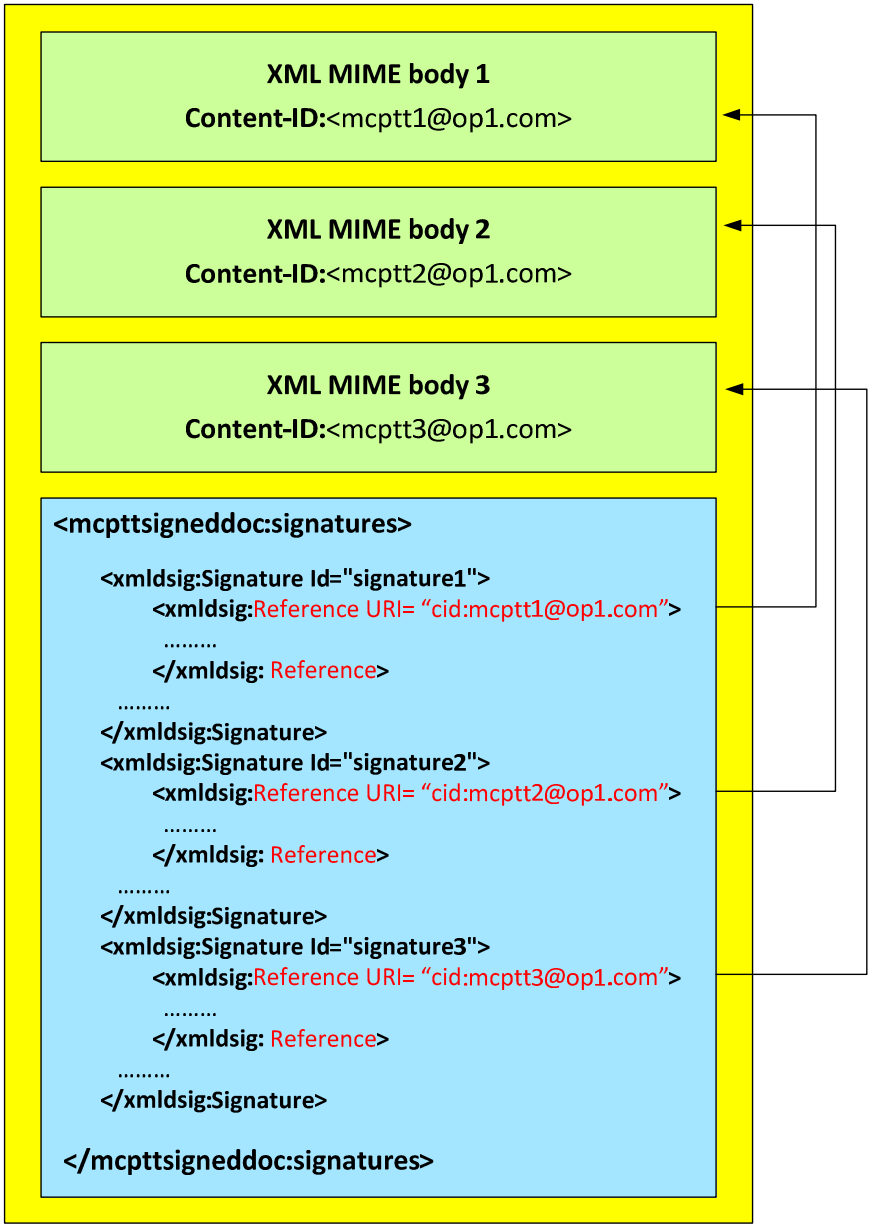

Figure 6.6.3.1-1: Integrity Protection of XML MIME bodies in SIP requests and SIP responses

Each MIME body that is integrity protected is assigned a unique signature.

When integrity protecting the XML content in SIP REFER request used for pre-established sessions, the application/vnd.3gpp.mcptt-signed+xml MIME type can appear twice in the SIP REFER request as illustrated in Figure 6.6.3.1-2.

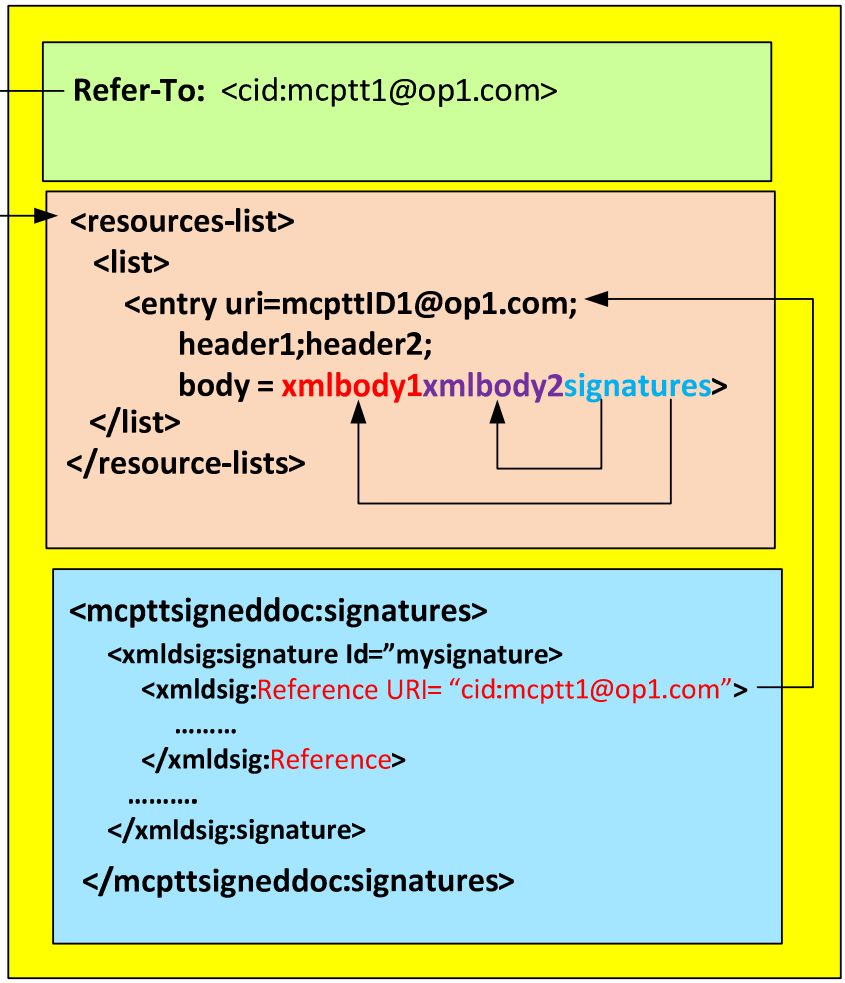

Figure 6.6.3.1-2: Integrity Protection of XML MIME bodies in SIP REFER requests

- an application/vnd.3gpp.mcptt-signed+xml MIME body is included in the SIP REFER request with a signature pointing to the application/resource-lists MIME body; and

NOTE 1: Sensitive XML content placed in the application/resource-lists MIME body can be encrypted.

- an application/vnd.3gpp.mcptt-signed+xml MIME is included in the hname "body" URI header field of the URI in the "uri" attribute of the <entry> element of the application/resource-lists MIME body in the SIP REFER request, containing signatures pointing to the XML MIME bodies included in the "body" URI header field.

NOTE 2: Sensitive XML content placed in the hname "body" URI header field can be encrypted.

Configuration for applying integrity protection is not selective to a specific MIME body. If configuration for integrity protection is turned on, then all XML MIME bodies in SIP requests and responses are integrity protected. If configuration for integrity protection is turned off, then no XML MIME bodies in SIP requests and SIP responses are integrity protected.

6.6.3.2 Keys used in integrity protection procedures

Integrity protection uses an XPK to sign the data which (depending on who is the sender and who is the receiver of the signed information) can be a CSK or an SPK as specified in subclause 4.8. An XPK-ID (CSK-ID/SPK-ID) is used to key the XPK (CSK/SPK). It is assumed that before the procedures in subclause 6.6.3.3 and subclause 6.6.3.4 are called, the CSK/CSK-ID and/or SPK/SPK-ID are available on the sender and recipient of the integrity protected content, as described in subclause 4.8.

The procedures in subclause 6.6.3.3 and subclause 6.6.3.4 shall be used with a XPK equal to the CSK and a XPK-ID equal to the CSK-ID in the following circumstances as described in 3GPP TS 33.180 [78]:

1) MCPTT client sends integrity protected content to an MCPTT server; and

2) MCPTT server sends integrity protected content to an MCPTT client.

The procedure in subclause 6.6.3.3 and subclause 6.6.3.4 shall be used with a XPK equal to the SPK and a XPK-ID equal to the SPK-ID in the following circumstances as described in 3GPP TS 33.180 [78]:

1) MCPTT server sends integrity protected content to an MCPTT server in the same domain; and

2) MCPTT server sends integrity protected content to an MCPTT server in another domain.

6.6.3.3 Sending integrity protected content

6.6.3.3.1 MCPTT client

If the <integrity-protection> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "true" or no <integrity-protection> element is present in the Service Configuration document, then sending integrity protected content from the MCPTT client to the MCPTT server is enabled, and the MCPTT client shall use the appropriate keying information specified in subclause 6.6.3.2 and shall perform the procedures in subclause 6.6.3.3.3 to integrity protect XML MIME bodies.

NOTE: Each XML MIME body is integrity protected separately.

If the <integrity-protection> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "false", then sending integrity protected content from the MCPTT client to the MCPTT server is disabled, and all XML MIME bodies are sent without integrity protection.

6.6.3.3.2 MCPTT server

If the <integrity-protection> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "true", or no <integrity-protection> element is present in the Service Configuration document, then sending integrity protected content from the MCPTT server to the MCPTT client is enabled. If the <allow-signalling-protection> element of the <protection-between-mcptt-servers> element is set to "true" in the Service Configuration document as specified in 3GPP TS 24.484 [50] or no <allow-signalling-protection> element is present in the Service Configuration document, then sending integrity protected content between MCPTT servers is enabled.

When sending integrity protected content, the MCPTT server shall use the appropriate keying information specified in subclause 6.6.3.2 and shall perform the procedures in subclause 6.6.3.3.3 to integrity protect XML MIME bodies.

NOTE: Each XML MIME body is integrity protected separately.

If the <integrity-protection> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "false", then sending integrity protected content from the MCPTT server to the MCPTT client is disabled, and all XML MIME bodies are sent without integrity protection.

If the <allow-signalling-protection> element of the <protection-between-mcptt-servers> element in the Service Configuration document as specified in 3GPP TS 24.484 [50] is set to "false", then sending integrity protected content between MCPTT servers is disabled, and content is included in XML elements without encryption.

6.6.3.3.3 Integrity protection procedure

The following procedure shall be performed by the MCPTT client and MCPTT server to integrity protect the XML bodies defined by the MIME types listed in subclause 6.6.3.1:

1) include a Content-Type header field set to "application/vnd.3gpp.mcptt-signed+xml";

2) for each of the MIME types defined in subclause 6.6.3.1 where the content defined by these MIME types is to be integrity protected:

   a) perform reference generation as specified in W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core [61] subclause 3.1.1 using the SHA256 algorithm to produce a hash of the MIME body and continue with the procedures below if reference generation is successful;

   b) perform signature generation as specified in W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core [61] subclause 3.1.2 using the HMAC-SHA256 signature

method and the XPK as the key and continue with the procedures below if signature generation is successful; and

3) follow the schema defined in Annex F.6.2 and the semantic described in Annex F.6.3 to create the application/vnd.3gpp.mcptt-signed+xml MIME body containing signatures referring to the XML MIME bodies included in the SIP request or SIP response.

6.6.3.4 Receiving integrity protected content

6.6.3.4.1 Determination of integrity protected content

The following procedure is used by the MCPTT client or MCPTT server to determine if an XML MIME body is integrity protected.

1) if the <Signature> XML element is not present in the XML MIME body, then the content is not integrity protected; and

2) if the <Signature> XML element is present in the XML MIME body, then the content is integrity protected.

6.6.3.4.2 Verification of integrity protected content

The following procedure is used by the MCPTT client or MCPTT server to verify the integrity of an XML MIME body:

1) if the required sub-elements of the <Signature> as described in 3GPP TS 33.180 [78] are not present in the MIME body and if not present, are not known to the sender and recipient by other means, then the integrity protection procedure fails and exit this procedure. Otherwise continue with the rest of the steps;

2) perform reference validation on the <Reference> element as specified in W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core [61] subclause 3.2.1;

3) if reference validation fails, then send a SIP 403 (Forbidden) response towards the functional entity with the warning text set to: "139 integrity protection check failed" in a Warning header field as specified in subclause 4.4, and do not continue with the rest of the steps in this subclause;

4) obtain the XPK using the XPK-ID in the received XML body and use it to perform signature validation of the value of the <SignatureValue> element as specified in W3C: "XML Signature Syntax and Processing (Second Edition)", http://www.w3.org/TR/xmldsig-core [61] subclause 3.2.2;

5) if signature validation fails, then send a SIP 403 (Forbidden) response towards the functional entity with the warning text set to: "139 integrity protection check failed" in a Warning header field as specified in subclause 4.4, and do not continue with the rest of the steps in this subclause; and

6) return success of the integrity protection of the XML document passes the integrity protection procedure.

6.7 Priority sharing

The participating MCPTT function shall enable or disable priority sharing as specified in 3GPP TS 24.229 [4].

7 Registration and service authorisation

7.1 General

This clause describes the procedures for SIP registration and MCPTT service authorization for the MCPTT client and the MCPTT service. The MCPTT UE can use SIP REGISTER or SIP PUBLISH for MCPTT service settings to perform service authorization for MCPTT. The decision which method to use is based on implementation and on availability of an access-token received as outcome of the user authentication procedure as described in 3GPP TS 24.482 [49].

If another MC service client (e.g. MCVideo, MCData) is operating at the same time on the same MC UE as the MCPTT client, then the MCPTT client shares the same SIP registration as the other MC service clients. The SIP REGISTER

procedures in this clause are combined with the SIP REGISTER procedures for the other operating MC service clients to create a single SIP REGISTER request. If other MC service clients are already operating when the MCPTT client registers, then a re-registration is performed containing the parameters for the other operating MC services.

Although the access-token can be the same for the MCPTT service as for other MC services when performing service authorization for MCPTT along with other MC services using SIP REGISTER multipart MIME bodies for each MC service are included in the SIP REGISTER request. The MCPTT server can therefore receive multipart MIME bodies in the SIP REGISTER request. Multiple contact addresses (one per MC service client) can be included in a SIP REGISTER request provided they all contain the same IP address and port number (see 3GPP TS 24.229 [4] for further details of including multiple contact addresses in a single SIP REGISTER request).

If the MCPTT client logs off from the MCPTT service but other MC service clients are to remain registered the MC UE performs a re-registration as specified in 3GPP TS 24.229 [4] without the g.3gpp.mcptt media feature tag and the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP REGISTER request but with the parameters for the remaining operating MC service clients.

7.2 MCPTT client procedures

7.2.1 SIP REGISTER request for service authorisation

When the MCPTT client performs SIP registration for service authorisation the MCPTT client shall perform the registration procedures as specified in 3GPP TS 24.229 [4].

The MCPTT client shall include the following media feature tags in the Contact header field of the SIP REGISTER request:

1) the g.3gpp.mcptt media feature tag; and

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

NOTE 1: If the MCPTT client logs off from the MCPTT service but the MCPTT UE remains registered the MCPTT UE performs a re-registration as specified in 3GPP TS 24.229 [4] without both the g.3gpp.mcptt media feature tag and the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP REGISTER request.

If the MCPTT client supports MCPTT service continuity, then the MCPTT client shall follow the IMS registraton procedures for PS to PS service continuity as specified in subclause 6.2.2 of 3GPP TS 24.237 [58].

If the MCPTT client, upon performing SIP registration:

1) has successfully finished the user authentication procedure as described in 3GPP TS 24.482 [49];

2) has available an access-token;

3) based on implementation decides to use SIP REGISTER for service authorization;

4) confidentiality protection is disabled as specified in subclause 6.6.2.3.1; and

5) integrity protection is disabled as specified in subclause 6.6.3.3.1;

then the MCPTT client shall include in the SIP REGISTER request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in Annex F.1 with:

1) the <mcptt-access-token> element set to the value of the access token received during the user authentication procedures; and

2) the <mcptt-client-id> element set to the value of the MCPTT client ID of the originating MCPTT client.

NOTE 2: the access-token contains the MCPTT ID of the user.

If the MCPTT client, upon performing SIP registration:

1) has successfully finished the user authentication procedure as described in 3GPP TS 24.482 [49];

2) has an available access-token;

3) based on implementation decides to use SIP REGISTER for service authorization; and

4) either confidentiality protection is enabled as specified in subclause 6.6.2.3.1 or integrity protection is enabled as specified in subclause 6.6.3.3.1;

then the MCPTT client:

1) shall include an application/mikey MIME body with the CSK as MIKEY-SAKKE I_MESSAGE as specified in 3GPP TS 33.180 [78] in the body of the SIP REGISTER request;

2) if confidentiality protection is enabled as specified in subclause 6.6.2.3.1, shall include in the body of the SIP REGISTER request, an application/vnd.3gpp.mcptt-info+xml MIME body with the following clarifications:

   a) shall encrypt the received access-token using the client server key (CSK) and include the <mcptt-access-token> element set to the encrypted access-token, as specified in subclause 6.6.2.3.3; and

   b) shall encrypt the MCPTT client ID of the originating MCPTT client and include the <mcptt-client-id> element set to the encrypted MCPTT client ID;

3) if confidentiality protection is disabled as specified in subclause 6.6.2.3.1, shall include an application/vnd.3gpp.mcptt-info+xml MIME body as defined in Annex F.1 with:

   a) the <mcptt-access-token> element set to the value of the access token received during the user authentication procedures; and

   b) the <mcptt-client-id> element set to the value of the MCPTT client ID of the originating MCPTT client; and

4) if integrity protection is enabled as specified in subclause 6.6.3.3.1, shall use the CSK to integrity protect the application/vnd.3gpp.mcptt-info+xml MIME body by following the procedures in subclause 6.6.3.3.3.

7.2.1AA SIP REGISTER request without service authorisation

When the MCPTT client performs SIP registration without service authorisation the MCPTT client shall perform the registration procedures as specified in 3GPP TS 24.229 [4].

The MCPTT client shall include the following media feature tags in the Contact header field of the SIP REGISTER request:

1) the g.3gpp.mcptt media feature tag; and

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

NOTE: If the MCPTT client logs off from the MCPTT service but the MCPTT UE remains registered the MCPTT UE performs a re-registration as specified in 3GPP TS 24.229 [4] without both the g.3gpp.mcptt media feature tag and the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP REGISTER request.

If the MCPTT client supports MCPTT service continuity, then the MCPTT client shall follow the IMS registraton procedures for PS to PS service continuity as specified in subclause 6.2.2 of 3GPP TS 24.237 [58].

7.2.1A Common SIP PUBLISH procedure

This procedure is only referenced from other procedures.

When populating the SIP PUBLISH request, the MCPTT client shall:

1) shall set the Request-URI to the public service identity identifying the participating MCPTT function serving the MCPTT user;

2) 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-Preferred-Service header field according to IETF RFC 6050 [9];

3) shall set the Event header field to the "poc-settings" value; and

4) shall set the Expires header field according to IETF RFC 3903 [37], to 4294967295, if the MCPTT user is not removing the MCPTT service settings, otherwise to remove the MCPTT service settings the MCPTT client shall set the Expires header field to zero.

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

NOTE 2: The expiration timer of the MCPTT client service settings is only applicable for the MCPTT client service settings from the MCPTT client that matches the Instance Identifier URN. The expiration timer of MCPTT user service settings is also updated in the MCPTT server if expiration timer of MCPTT client service settings is updated in the MCPTT server.

NOTE 3: Removing the MCPTT service settings by setting the Expires header field to zero, logs off the MCPTT client from the MCPTT service.

7.2.2 SIP PUBLISH request for service authorisation and MCPTT service settings

If based on implementation the MCPTT client decides to use SIP PUBLISH for MCPTT server settings to also perform service authorization and

1) has successfully finished the user authentication procedure as described in 3GPP TS 24.482 [49]; and

2) has available an access-token;

then the MCPTT client:

1) shall perform the procedures in subclause 7.2.1A;

2) if confidentiality protection is disabled as specified in subclause 6.6.2.3.1 and integrity protection is disabled, shall include in the body of the SIP PUBLISH request, an application/vnd.3gpp.mcptt-info+xml MIME body as specified in Annex F.1 with the <mcptt-access-token> element set to the value of the access token received during the user authentication procedures;

3) if either confidentiality protection is enabled as specified in subclause 6.6.2.3.1 or integrity protection is enabled as specified in subclause 6.6.3.3.1 shall include an application/mikey MIME body with the CSK as MIKEY-SAKKE I_MESSAGE as specified in 3GPP TS 33.180 [78] in the body of the SIP PUBLISH request;

4) if confidentiality protection is enabled as specified in subclause 6.6.2.3.1, shall include in the body of the SIP PUBLISH request an application/vnd.3gpp.mcptt-info+xml MIME body with:

   a) the <mcptt-access-token> element set to the received access-token encrypted using the CSK, as specified in subclause 6.6.2.3.3; and

   b) the <mcptt-client-id> element set to the encrypted MCPTT client ID of the originating MCPTT client, as specified in subclause 6.6.2.3.3;

5) if confidentiality protection is disabled as specified in subclause 6.6.2.3.1, shall include in the body of the SIP PUBLISH request, an application/vnd.3gpp.mcptt-info+xml MIME body as specified in Annex F.1 with:

   a) the <mcptt-access-token> element set to the value of the access token received during the user authentication procedures in the body of the SIP PUBLISH request; and

   b) the <mcptt-client-id> element set to the value of the MCPTT client ID of the originating MCPTT client;

6) shall include an application/poc-settings+xml MIME body containing:

   a) the Answer-Mode Indication setting in the <am-settings> element of the poc-settings event package set to the current answer mode setting ("auto-answer" or "manual-answer") of the MCPTT client according to IETF RFC 4354 [55]; and

   b) the <selected-user-profile-index> element as defined in subclause 7.4.1.2.2 set to the value contained in the "user-profile-index" attribute of the selected MCPTT user profile as defined in 3GPP TS 24.484 [50]; and

7) if integrity protection is enabled as specified in subclause 6.6.3.3.1, shall use the CSK to integrity protect the application/vnd.3gpp.mcptt-info+xml MIME body and application/poc-settings+xml MIME body by following the procedures in subclause 6.6.3.3.3.

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

7.2.3 Sending SIP PUBLISH for MCPTT service settings only

To set, update, remove or refresh the MCPTT service settings, the MCPTT client shall generate a SIP PUBLISH request according 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 4354 [55]. In the SIP PUBLISH request, the MCPTT client:

1) shall perform the procedures in subclause 7.2.1A;

2) if confidentiality protection is enabled as specified in subclause 6.6.2.3.1, shall include in the body of the SIP PUBLISH request, an application/vnd.3gpp.mcptt-info+xml MIME body with:

   a) the <mcptt-request-uri> element set to the targeted MCPTT ID encrypted using the CSK, as specified in subclause 6.6.2.3.3; and

   b) the <mcptt-client-id> element set to the encrypted MCPTT client ID of the originating MCPTT client, as specified in subclause 6.6.2.3.3;

3) if confidentiality protection is disabled as specified in subclause 6.6.2.3.1, shall include an application/vnd.3gpp.mcptt-info+xml MIME body as specified in Annex F.1 with:

   a) the <mcptt-request-uri> set to the cleartext targeted MCPTT ID; and

   b) the <mcptt-client-id> element set to the value of the MCPTT client ID of the originating MCPTT client;

4) shall include an application/poc-settings+xml MIME body containing:

   a) the Answer-Mode Indication setting in the <am-settings> element of the poc-settings event package set to the current answer mode setting ("auto-answer" or "manual-answer") of the MCPTT client according to IETF RFC 4354 [55]; and

   b) the <selected-user-profile-index> element as defined in subclause 7.4.1.2.2 set to the value contained in the "user-profile-index" attribute of the selected MCPTT user profile as defined in 3GPP TS 24.484 [50]; and

5) if integrity protection is enabled as specified in subclause 6.6.3.3.1, shall use the CSK to integrity protect the application/vnd.3gpp.mcptt-info+xml MIME body and application/poc-settings+xml MIME body by following the procedures in subclause 6.6.3.3.3.

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

On receiving the SIP 200 (OK) response to the SIP PUBLISH request the MCPTT client may indicate to the MCPTT User the successful communication of the MCPTT service settings to the MCPTT server.

7.2.4 Determination of MCPTT service settings

In order to discover MCPTT service settings of another MCPTT client of the same MCPTT user or to verify the currently active MCPTT service settings of this MCPTT client, the MCPTT client shall generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 6665 [26], and IETF RFC 4354 [55].

In the SIP SUBSCRIBE request, the MCPTT client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall include the <mcptt-request-uri> element set to the MCPTT ID of the MCPTT user;

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-Preferred-Service header field according to IETF RFC 6050 [9];

4) shall set the Event header field to the 'poc-settings' value;

5) shall include an Accept header field containing the "application/poc-settings+xml" MIME type;

6) if the MCPTT client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295; and

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

7) if the MCPTT client wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [26], to zero.

In order to re-subscribe or de-subscribe, the MCPTT client shall generate an in-dialog SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 6665 [26], IETF RFC 4354 [55]. In the SIP SUBSCRIBE request, the MCPTT client:

1) shall set the Event header field to the 'poc-settings' value;

2) shall include an Accept header field containing the "application/poc-settings+xml" MIME type;

3) if the MCPTT client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295; and

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

4) if the MCPTT client wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [26], to zero.

Upon receiving a SIP NOTIFY request according to 3GPP TS 24.229 [4], IETF RFC 6665 [26] and IETF RFC 4354 [55], that contains an application/poc-settings+xml MIME body the MCPTT client shall cache:

1) the <am-settings> element of the poc-settings+xml MIME body for each MCPTT client identified by the "id" attribute according to IETF RFC 4354 [55] as the current Answer-mode indication of that MPCTT client; and

2) the <selected-user-profile-index> element of the poc-settings+xml MIME body for each MCPTT client identified by the "id" attribute according to IETF RFC 4354 [55] as the active MCPTT service user profile of that MCPTT client.

7.2.5 Receiving a CSK key download message

When the MCPTT client receives a SIP MESSAGE request containing:

1) a P-Asserted-Service header field containing the "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

2) an application/mikey MIME body;

Then, if the key identifier within the CSB-ID of the MIKEY payload is a CSK-ID (4 most-significant bits have the value '2'), the MCPTT client:

1) shall follow the security procedures in subclause 9.2.1 of 3GPP TS 33.180 [78] to extract the CSK. The client:

   a) if the initiator field (IDRi) has type 'URI' (identity hiding is not used), the client:

      i) shall extract the initiator URI from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]. If the initiator URI deviates from the public service identity of the participating MCPTT function serving the MCPTT user, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

      ii) shall convert the initiator URI to a UID as described in 3GPP TS 33.180 [78];

   b) if the initiator field (IDRi) has type 'UID' (identity hiding in use), the client:

ii) shall convert the public service identity of participating MCPTT function serving the MCPTT user to a UID as described in 3GPP TS 33.180 [78];

i) shall compare the generated UID with the UID in the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]. If the two initiator UIDs deviate from each other, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

c) shall use the UID to validate the signature of the I_MESSAGE as described in 3GPP TS 33.180 [78];

d) if authentication verification of the I_MESSAGE fails, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

e) shall extract and decrypt the encapsulated CSK using the participating MCPTT function's (KMS provisioned) UID key as described in 3GPP TS 33.180 [78]; and

f) shall extract the CSK-ID, from the payload as specified in 3GPP TS 33.180 [78];

2) Upon successful extraction, the client shall replace the existing CSK and CSK-ID associated with the participating MCPTT function, with the extracted CSK and CSK-ID in the 'key download' message.

7.3 MCPTT server procedures

7.3.1 General

The MCPTT server obtains information that it needs to implement service authorization specific requirements from:

a) any received third-party SIP REGISTER request (e.g. including information contained in the body of the third-party SIP REGISTER request) as specified in 3GPP TS 24.229 [4]. The body will carry the SIP REGISTER request as sent by the MCPTT client and may contain information needed for service authorization; or

b) any received SIP PUBLISH request for MCPTT server settings containing the g.3gpp.mcptt media feature tag along with the "require" and "explicit" header field parameters. The body of the SIP PUBLISH request will contain information needed for service authorization.

7.3.1A Confidentiality and Integrity Protection

When the MCPTT server receives a SIP REGISTER request sent from the MCPTT client contained within a message/sip MIME body of a received third-party SIP REGISTER request or a SIP PUBLISH request, it first determines whether XML MIME bodies included in the request are integrity protected. If XML MIME bodies are integrity protected the MCPTT server validates the signature of each of the XML MIME bodies. If the integrity protection check(s) pass or the XML MIME bodies are not integrity protected, the MCPTT server then determines whether the content in specific XML elements is confidentiality protected. If XML content is confidentiality protected, the MCPTT server decrypts the protected content.

Upon receiving:

- a SIP REGISTER request containing an application/vnd.3gpp.mcptt-info+xml MIME body within a message/sip MIME body of the SIP REGISTER request sent from the MCPTT client; or

- a SIP PUBLISH request containing an application/vnd.3gpp.mcptt-info+xml MIME body and an application/poc-settings+xml MIME body;

the MCPTT server:

1) shall determine if integrity protection has been applied to XML MIME bodies in the SIP request by following the procedures in subclause 6.6.3.4.1 for each XML MIME body;

2) if integrity protection has been applied, shall use the keying data described in subclause 6.6.3.2 and the procedures described in subclause 6.6.3.4.2 to verify the integrity of each of the XML MIME bodies; and

3) if all integrity protection checks succeed, shall continue with the remaining steps of this subclause.

Upon receiving:

- a SIP REGISTER request 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; or

- a SIP PUBLISH request containing an application/vnd.3gpp.mcptt-info+xml MIME body with an <mcptt-access-token> element and an <mcptt-client-id> element, and an application/poc-settings+xml MIME body;

the MCPTT server:

1) shall determine if confidentiality protection has been applied to the <mcptt-access-token> element and the <mcptt-client-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body, by following the procedures in subclause 6.6.2.4.1;

2) if confidentiality protection has been applied to the <mcptt-access-token> element and <mcptt-client-id> element:

   a) shall use the keying information received in the MIKEY-SAKKE I_MESSAGE as specified in 3GPP TS 33.180 [78], along with the procedures described in subclause 6.6.2.4.2 to:

      i) decrypt the received access token in the <mcptt-access-token> element in the application/vnd.3gpp.mcptt-info+xml MIME body; and

      ii) decrypt the received MCPTT client ID in the <mcptt-client-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body;

   b) if the decryption procedure succeeds, shall identify the MCPTT ID and the MCPTT client ID from the decrypted values; and

   c) if the decryption procedure fails, shall determine that confidentiality protection has not been successful;

3) if confidentiality protection has been applied to only one of the <mcptt-access-token> element or the <mcptt-client-id> element:

   a) shall determine that confidentiality protection has not been successful;

4) if confidentiality protection has not been applied:

   a) shall identify the MCPTT ID from <mcptt-access-token> element received in the application/vnd.3gpp.mcptt-info+xml MIME body; and

   b) shall identify the MCPTT client ID from the <mcptt-client-id> element received in the application/vnd.3gpp.mcptt-info+xml MIME body.

Upon receiving a SIP PUBLISH request containing an application/vnd.3gpp.mcptt-info+xml MIME body with an <mcptt-request-uri> element, an <mcptt-client-id> element, and an application/poc-settings+xml MIME body, the MCPTT server:

1) shall determine if confidentiality protection has been applied to the <mcptt-request-uri> element and the <mcptt-client-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body by following the procedures in subclause 6.6.2.4.1;

2) if confidentiality protection has been applied to the <mcptt-request-uri> element and the <mcptt-client-id> element:

   a) shall use the keying information described in subclause 6.6.2.2 along with the procedures described in subclause 6.6.2.4.2 to:

      i) decrypt the received encrypted MCPTT ID in the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body; and

      ii) decrypt the received encrypted MCPTT client ID in the <mcptt-client-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body;

b) if all decryption procedures succeed, shall identify the MCPTT ID and MCPTT client ID from the decrypted values; and

c) if the decryption procedure fails, shall determine that confidentiality protection has not been successful;

3) if confidentiality protection has been applied to only one of the <mcptt-request-uri> element or <mcptt-client-id> element:

a) shall determine that confidentiality protection has not been successful;

4) if confidentiality protection has not been applied:

a) shall identify the MCPTT ID from the contents of the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body;and

b) shall identify the MCPTT client ID from the <mcptt-client-id> element received in the application/vnd.3gpp.mcptt-info+xml MIME body.

7.3.2 SIP REGISTER request for service authorisation

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 33.180 [78];

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.

7.3.3 SIP PUBLISH request for service authorisation and service settings

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 33.180 [78];

5) if service authorization was successful:

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

   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.

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];

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.

11) 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 and use the <selected-user-profile-index> element of the poc-settings event package if included to identify the active MCPTT user profile for the MCPTT client;

NOTE 2: If the <selected-user-profile-index> element of the poc-settings event package is included then only that MCPTT user profile is needed to be downloaded from the MCPTT user database.

12) if there is no <selected-user-profile-index> element included in the poc-settings event package then 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 to be used as the active MCPTT user profile by identifying the MCPTT user profile (see the MCPTT user profile document in 3GPP TS 24.484 [50]) in the collection of MCPTT user profiles that contains a <Pre-selected-indication> element; and

NOTE 3: 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.

13) 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 24.484 [50]) for the served MCPTT ID, shall perform implicit affiliation as specified in subclause 9.2.2.2.15

7.3.4 Receiving SIP PUBLISH request for MCPTT service settings only

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 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;

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];

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.

11) 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 and use the <selected-user-profile-index> element of the poc-settings event package if included to identify the active MCPTT user profile for the MCPTT client;

NOTE 1: If the <selected-user-profile-index> element of the poc-settings event package is included then only that MCPTT user profile is needed to be downloaded from the MCPTT user database.

12) if there is no <selected-user-profile-index> element included in the poc-settings event package then 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 to be used as the active MCPTT user profile by identifying the MCPTT user profile (see the MCPTT user profile document in 3GPP TS 24.484 [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.

13) 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 24.484 [50]) for the served MCPTT ID, shall perform implicit affiliation as specified in subclause 9.2.2.2.15.

7.3.5 Receiving SIP PUBLISH request with "Expires=0"

Upon receiving a SIP PUBLISH request containing:

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

2) an Expires header field set to 0;

the MCPTT server:

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

2) shall process the SIP PUBLISH request according to rules and procedures of IETF RFC 3903 [37] and if processing of the SIP request was successful, continue with the rest of the steps;

3) shall remove the MCPTT service settings;

4) shall remove the binding between the MCPTT ID and public user identity; and

5) shall send a SIP 200 (OK) response according to 3GPP TS 24.229 [4].

7.3.6 Subscription to and notification of MCPTT service settings

7.3.6.1 Receiving subscription to MCPTT service settings

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the participating MCPTT function of the served MCPTT user;

2) the SIP SUBSCRIBE request contains an application/vnd.3gpp.mcptt-info+xml MIME body containing the<mcptt-request-uri> element which identifies an MCPTT ID served by the MCPTT server;

3) 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 header field according to IETF RFC 6050 [9]; and

3) the Event header field of the SIP SUBSCRIBE request contains the 'poc-settings' event type.

the MCPTT server:

1) shall identify the served MCPTT ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP SUBSCRIBE request;

2) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the participating MCPTT function serving the MCPTT user, shall identify the originating MCPTT ID from public user identity in the P-Asserted-Identity header field of the SIP SUBSCRIBE request;

3) if the originating MCPTT ID is different than the served MCPTT ID, shall send a 403 (Forbidden) response and shall not continue with the rest of the steps; and

4) shall generate a 200 (OK) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 6665 [26] and IETF RFC 4354 [55].

For the duration of the subscription, the MCPTT server shall notify subscriber about changes of the MCPTT service settings of the subscribed MCPTT user, as described in subclause 7.3.6.2.

7.3.6.2 Sending notification of change of MCPTT service settings

In order to notify the subscriber about changes of the MCPTT service settings of the subscribed MCPTT client of the subscribed MCPTT user, the MCPTT server:

1) shall generate an application/poc-settings+xml MIME body containing:

   a) the <am-settings> element of the poc-settings event package set to the current answer mode setting of the MCPTT client according to IETF RFC 4354 [55]; and

   b) the <selected-user-profile-index> element as defined in subclause 7.4.1.2.2 identifying the active MCPTT user profile; and

2) send a SIP NOTIFY request according to 3GPP TS 24.229 [4], IETF RFC 6665 [26] and IETF RFC 4354 [55] with the constructed application/poc-settings+xml MIME body.

7.3.7 Sending a CSK key download message

If confidentiality protection is enabled as specified in subclause 6.6.2.3.1, and if the participating MCPTT function received a Client Server Key (CSK) within a SIP REGISTER request for service authorisation or SIP PUBLISH request for service authorisation, the participating MCPTT function may decide to update the CSK. In this case, the participating MCPTT function shall perform a key download procedure for the CSK. The participating MCPTT function:

1) shall generate an SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

2) shall set the Request-URI to the URI received in the To header field in a third-party SIP REGISTER request;

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

4) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

5) shall include an application/mikey MIME body containing the CSK-ID and the CSK encrypted within a MIKEY message to the MC client as specified in clause 9.2.1 of 3GPP TS 33.180 [78] in the body of the SIP MESSAGE request;

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

7.4 Coding

7.4.1 Extension of MIME types

7.4.1.1 General

The parent subclause of this subclause defines extensions of MIME type defined in other documents.

7.4.1.2 Extension of application/poc-settings+xml MIME type

7.4.1.2.1 Introduction

The parent subclause of this subclause describes extension of the application/poc-settings+xml MIME body specified in IETF RFC 4354 [55]. The extension is used to indicate the selected MCS user profile at an MC client.

7.4.1.2.2 Syntax

The application/poc-settings+xml MIME body indicating the selected MCS user profile at an MC client is constructed according to IETF RFC 4354 [55] and:

1) contains a <poc-settings> root element according to IETF RFC 4354 [55];

2) contains one or more <entity> child element according to IETF RFC 4354 [55] of the <poc-settings> element;

3) contains one <selected-user-profile-index> child element defined in the XML schema defined in table 7.4.1.2.2-2, of the <entity> element;

NOTE: The <selected-user-profile-index> element is validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <entity> element.

The application/poc-settings+xml MIME body refers to namespaces using prefixes specified in table 7.4.1.2.2-1.

Table 7.4.1.2.2-1: Assignment of prefixes to namespace names in the application/poc-settings+xml MIME body

Prefix	Namespace
PoC1Set	urn:oma:params:xml:ns:poc:poc-settings
mcs10Set	urn:3gpp:mcsSettings:1.0

Table 7.4.1.2.2-2: XML schema with elements and attributes extending the application/poc-settings+xml MIME body

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:3gpp:mcsSettings:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:mcs10Set="urn:3gpp:mcsSettings:1.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <!-- MCS specific "entity" child elements -->
  <xs:element name="selected-user-profile-index" type="mcs10Set:selected-user-profile-indexType"/>

  <xs:complexType name="selected-user-profile-indexType">
    <xs:sequence>
      <xs:element name="user-profile-index" type="xs:nonNegativeInteger"/>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

</xs:schema>
```

An example application/poc-settings+xml MIME body showing the MC service settings for two MC clients as might be included in the body of a SIP NOTIFY request is shown in table 7.4.1.2.2-3.

Table 7.4.1.2.2-3: Example application/poc-settings+xml MIME body showing the MC service settings for two MC clients as might be included in the body of a SIP NOTIFY request

```
<?xml version="1.0" encoding="UTF-8"?>
   <poc-settings xmlns="urn:oma:params:xml:ns:poc:poc-settings">
     <entity id="urn:uuuid:do39s8zksn2d98x">
        <am-settings>
          <answer-mode>automatic</answer-mode>
        </am-settings>
        <selected-user-profile-index>
          <user-profile-index>1</user-profile-index>
        </selected-user-profile-index>
     </entity>
     <entity id="urn:uuuid:ksn2d98xdo39s8z">
        <am-settings>
          <answer-mode>manual</answer-mode>
        </am-settings>
        <selected-user-profile-index>
          <user-profile-index>2</user-profile-index>
        </selected-user-profile-index>
     </entity>
   </poc-settings>
```

8 Pre-established session

8.1 General

The MCPTT client may establish one or more pre-established sessions to the participating MCPTT function at any time after SIP registration and setting the service settings as defined in subclause 7.2.2 or subclause 7.2.3.

The MCPTT client may use the pre-established session for originating MCPTT calls after pre-established session establishment.

The participating MCPTT function may use the pre-established session for terminating MCPTT calls after pre-established session establishment.

The MCPTT client may initiate the modification of the media parameters of a pre-established session as defined in subclause 8.3.1.1.

The participating MCPTT function may initiate the modification of the media parameters of a pre-established session as defined in subclause 8.3.2.2.

The MCPTT client may initiate the release of a pre-established session as defined in subclause 8.4.1.1.

The participating MCPTT function may initiate the release of a pre-established session as defined in subclause 8.4.2.2.

The use of a pre-established session requires the use of resource sharing as specified in 3GPP TS 29.214 [79] and 3GPP TS 24.229 [4] by the participating MCPTT function. The participating MCPTT function use of resource sharing is defined in subclause 8.1A.

8.1A Participating MCPTT function use of resource sharing

The participating MCPTT function utilises resource sharing either:

1) via the SIP core as specified in 3GPP TS 24.229 [4]; or

2) by directly interfacing to PCC to control resource sharing via the Rx reference point as specified in 3GPP TS 29.214 [79].

If resource sharing is supported then the participating MCPTT function shall allow the use of pre-established sessions by the MCPTT client.

The participating MCPTT function can determine that the SIP core supports resource sharing from:the received third-party SIP REGISTER request if the Resource-Share header field with the value "supported" is contained in the "message/sip" MIME body of the third-party SIP REGISTER request as specified in 3GPP TS 24.229 [4].

When using resource sharing the participating MCPTT function uses the "+g.3gpp.registration-token" header field parameter in the Contact header field of the third-party REGISTER request to identify the MCPTT UE that is registering and to identify whether resource sharing and pre-established sessions can be used with a specific MCPTT UE.

8.2 Session establishment

8.2.1 MCPTT client procedures

When the MCPTT client initiates a pre-established session the MCPTT client shall:

1) gather ICE candidates according to IETF RFC 5245 [17]; and

NOTE 1: ICE candidates are only gathered on interfaces that the MCPTT UE uses to obtain MCPTT service.

2) generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) shall set the Request-URI of the SIP INVITE request to the public service identity of the participating MCPTT function serving the MCPTT user;

2) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [4];

3) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

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

5) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP INVITE request;

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

7) shall include the "timer" option tag in the Supported header field;

8) should include the Session-Expires header field according to IETF RFC 4028 [7] and should not include the "refresher" header field. The "refresher" header field parameter shall be set to "uac" if included;

9) shall include an SDP offer according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.1, and include ICE candidates in the SDP offer as per IETF RFC 5245 [17]; and

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

Upon receiving a SIP 2xx response to the SIP INVITE request the MCPTT client:

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

NOTE 2: If ICE candidate evaluation results in candidate pairs other than the default candidate pair being selected a further offer answer exchange using the procedures in subclause 8.3 will be needed.

8.2.2 Participating MCPTT function procedures

Upon receipt of a "SIP INVITE request for establishing a pre-established session" the participating MCPTT function:

1) shall check whether the public service identity is allocated and perform the actions specified in subclause 6.3.7.1 if it is not allocated. Otherwise, continue with the rest of the steps;

2) shall determine the MCPTT ID of the MCPTT user establishing the pre-established session and perform actions to verify the MCPTT ID of the MCPTT client and authorise the request according to local policy, and if not authorised, the participating MCPTT function shall return a SIP 403 (Forbidden) response with the warning text set to "100 function not allowed due to <detailed reason>" as specified in subclause 4.4. Otherwise, continue with the rest of the steps;

3) shall determine whether resource sharing is supported (see subclause 8.1A);

4) if resource sharing is supported by the SIP core, determine that there is a binding between the MCPTT ID of the MCPTT user establishing the pre-established session and the MCPTT UE identified by the "+g.3gpp.registration-token" header field parameter in the Contact header field of the third-party REGISTER request (see subclause 8.1A) and that this UE identity matches the identity in the "+g.3gpp.registration-token" header field parameter in the Feature-Caps header field in the "SIP INVITE request for establishing a pre-established session";

5) if resource sharing is not supported or if there is no binding between the MCPTT ID of the MCPTT user and the identity of the MCPTT UE identified by the "+g.3gpp.registration-token" header field parameter in the Feature-Caps header field,then the participating MCPTT function shall return a SIP 403 (Forbidden) response with the warning text set to "100 function not allowed due to pre-established session not supported" as specified in subclause 4.4 and not continue with the rest of the steps;

6) 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;

7) shall verify that the media resources are available to support the media parameters and if not shall reject the request with a SIP 500 (Server Internal Error) response, and shall not continue with the rest of the steps;

8) shall allocate a URI to be used to identify the pre-established session;

9) shall generate a SIP 200 (OK) response to the SIP INVITE request according to subclause 6.3.2.1.5.2; and

   a) shall include a Contact header field containing the URI that identifies the pre-established session;

   b) shall include the public service identity in the P-Asserted-Identity header field;

   c) shall include a Supported header field containing the "norefersub" option tag;

   d) shall if the SIP core supports resource sharing, include a Resource-Share header field answer as specified in 3GPP TS 24.229 [4] with:

      A) the value "media-sharing";

      B) an "origin" header field parameter set to "session-initiator";

      C) a "timestamp" header field parameter; and

      D) a "rules" header field parameter with one resource sharing rule per media stream in the same order the corresponding m-line appears in the SDP. Each resource sharing rule is constructed as follows:

         - a "new-sharing-key" part; and

         - a "directionality" part indicating the direction of the pre-established media stream; and

   e) shall include an SDP answer as specified in 3GPP TS 24.229 [4] with the clarifications in subclause 6.3.2.1.2.2 and include ICE candidates in the SDP answer as per IETF RFC 5245 [17];

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

NOTE 1: Resulting media plane processing is completed before the next step is performed.

11) shall send the SIP 200 (OK) response towards the MCPTT client according to the rules and procedures of the 3GPP TS 24.229 [4]; and

12) shall evaluate the ICE candidates according to IETF RFC 5245 [17].

NOTE 2: If ICE candidate evaluation results in candidate pairs other than the default candidate pair being selected a further offer answer exchange using the procedures in subclause 8.3 will be needed.

8.3 Session modification

8.3.1 MCPTT client procedures

8.3.1.1 MCPTT client initiated

When the MCPTT client needs to modify the pre-established session outside of an MCPTT session, the MCPTT client:

1) shall generate a SIP UPDATE request or a SIP re-INVITE request according to 3GPP TS 24.229 [4];

2) shall include an SDP offer according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.1, and include ICE candidates in the SDP offer as per IETF RFC 5245 [17], if required; and

3) shall send the SIP request towards the MCPTT server according to rules and procedures of 3GPP TS 24.229[4].

On receipt of the SIP 200 (OK) response the MCPTT client:

1) shall interact with media plane as specified in 3GPP TS 24.380 [5], if there is change in media parameters or codecs in the received SDP answer, compared to those in the previously agreed SDP; and

2) shall interact with media plane as specified in 3GPP TS 24.380 [5], if there is a media stream, that is currently used in the pre-established session, marked as rejected in the received SDP answer.

NOTE: The MCPTT client keeps resources for previously agreed media stream, media parameters and codecs until it receives a SIP 200 (OK) response.

8.3.1.2 Participating MCPTT function initiated

Upon receiving a SIP UPDATE request or a SIP re-INVITE request to modify an existing pre-established session without associated MCPTT session, the MCPTT client:

1) shall validate that the received SDP offer includes at least one media stream for which the media parameters and at least one codec is acceptable by the MCPTT client and if not reject the request with a SIP 488 (Not Acceptable Here) response. Otherwise, continue with the rest of the steps; and

2) shall generate a SIP 200 (OK) response as follows:

   a) shall include an SDP answer according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.2, and include ICE candidates in the SDP answer as per IETF RFC 5245 [17]. if required.

8.3.2 Participating MCPTT function procedures

8.3.2.1 MCPTT client initiated

Upon receiving a SIP UPDATE request or a SIP re-INVITE request to modify an existing pre-established session without associated MCPTT session, the participating MCPTT function:

1) shall validate that the received SDP offer includes at least one media stream for which the media parameters and at least one codec is acceptable by the participating MCPTT function and if not reject the request with a SIP 488 (Not Acceptable Here) response. Otherwise, continue with the rest of the steps; and

2) shall generate a SIP 200 (OK) response as follows:

   a) include an SDP answer according to 3GPP TS 24.229 [4] based on the received SDP offer with the clarifications given in the 6.3.2.1.2.2, and include ICE candidates in the SDP answer as per IETF RFC 5245 [17], if required; and

   b) include a Contact header field containing the URI that identifies the pre-established session and send a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229[4].

8.3.2.2 Participating MCPTT function initiated

When the participating MCPTT function needs to modify the pre-established session outside of an MCPTT session, the participating MCPTT function:

1) shall generate a SIP UPDATE request or a SIP re-INVITE request according to 3GPP TS 24.229 [4];

2) shall include an SDP offer according to 3GPP TS 24.229 [4], and include ICE candidates in the SDP offer as per IETF RFC 5245 [17], if required;

3) shall interact with the media plane as specified in 3GPP TS 24.380 [5], if removing a media-floor control entity; and

4) shall send the SIP request towards the MCPTT client according to rules and procedures of 3GPP TS 24.229[4].

On receipt of the SIP 200 (OK) response the participating MCPTT function:

1) shall interact with media plane as specified in 3GPP TS 24.380 [5], if there is change in media parameters or codecs in the received SDP answer, compared to those in the previously agreed SDP;

2) shall interact with media plane as specified in 3GPP TS 24.380 [5], if there is a media stream, that is currently used in the pre-established session, marked as rejected in the received SDP answer; and

3) shall interact with media plane as specified in 3GPP TS 24.380 [5], if there is a media stream accepted in the received SDP answer, that is not currently used by the participant in the pre-established session.

NOTE: The participating MCPTT function keeps resources for previously agreed media stream, media-floor control entities, media parameters and codecs until it receives a SIP 200 (OK) response.

8.4 Session release

8.4.1 MCPTT client procedures

8.4.1.1 MCPTT client initiated

NOTE: The MCPTT client needs to be prepared to release the pre-established session when receiving a SIP BYE request generated by the SIP core (e.g. due to network release of media plane resources).

When a MCPTT client needs to release a pre-established session as created in subclause 8.2.1, the MCPTT client:

1) shall generate a SIP BYE request according to rules and procedures of 3GPP TS 24.229 [4];

2) shall set the Request-URI of the SIP BYE request to the URI that identifies the pre-established session;

3) shall send the SIP BYE request towards the participating MCPTT function within the SIP dialog of the pre-established session according to rules and procedures of the 3GPP TS 24.229 [4]; and

4) shall, upon receiving a SIP 200 (OK) response to the SIP BYE request interact with the media plane as specified in 3GPP TS 24.380 [5].

8.4.1.2 Participating MCPTT function initiated

Upon receiving a SIP BYE request from the participating MCPTT function within a pre-established session the MCPTT client shall check whether there are any MCPTT sessions using the pre-established session, and:

1) if there is an established MCPTT session then the MCPTT client shall remove the MCPTT client from the MCPTT session by performing the procedures for session release for each MCPTT session as specified in 3GPP TS 24.380 [5]; and

2) if there is no MCPTT session using the pre-established session, then the MCPTT client shall:

   a) interact with the media plane as specified in 3GPP TS 24.380 [5] for disconnecting the media plane resources towards the participating MCPTT function; and

   b) shall generate and send a SIP 200 (OK) response to the SIP BYE request according to rules and procedures of 3GPP TS 24.229 [4].

8.4.2 Participating MCPTT function procedures

8.4.2.1 MCPTT client initiated

Upon receiving a SIP BYE request from the MCPTT client within a pre-established session the participating MCPTT function:

1) shall check whether there is a MCPTT session using the pre-established session, and:

   a) if there is an established MCPTT session then the participating MCPTT function shall remove the MCPTT client from the MCPTT session by performing the procedures as specified in subclause 6.3.2.1.6; and

   b) if there is a MCPTT session in the process of being established, then the participating MCPTT function:

      i) shall send a SIP CANCEL request to cancel the MCPTT session in the process of being established as specified in 3GPP TS 24.229 [4]; and

      ii) shall release the MCPTT session as specified in the subclause subclause 6.3.2.1.6, if a SIP 200 (OK) response for the SIP INVITE request is received from the remote side; and

   c) if there is no MCPTT session using the pre-established session, then the participating MCPTT function shall:

      i)_ interact with the media plane as specified in 3GPP TS 24.380 [5] for disconnecting the media plane resources towards the MCPTT client; and

ii) shall generate and send a SIP 200 (OK) response to the SIP BYE request according to rules and procedures of 3GPP TS 24.229 [4].

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

1) shall interact with the media plane as specified in 3GPP TS 24.380 [5] for releasing media plane resources towards the remote side;

2) shall interact with the media plane as specified in 3GPP TS 24.380 [5] for releasing media plane resources towards the MCPTT client; and

3) shall send a SIP 200 (OK) response to the SIP BYE request to the MCPTT client.

8.4.2.2 Participating MCPTT function initiated

When a participating MCPTT function needs to release a pre-established session as created in subclause 8.2.2, the participating MCPTT function:

1) shall first release any participants of all MCPTT calls that are using the pre-established session using the procedures as follows. The participating MCPTT function:

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

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

   c) shall set the Request-URI to the MCPTT session identity;

   d) shall set the contents of the P-Asserted-Identity header field to the P-Asserted-Identity header field of the MCPTT client that's pre-established session is being release;

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

   f) shall, upon receiving a SIP 200 (OK) response to the SIP BYE request the terminating MCPTT function 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 according to rules and procedures of 3GPP TS 24.229 [4];

3) shall set the Request-URI of the SIP BYE request to the URI that identifies the pre-established session;

4) shall send the SIP BYE request towards the MCPTT client within the SIP dialog of the pre-established session according to rules and procedures of the 3GPP TS 24.229 [4]; and

5) shall, upon receiving a SIP 200 (OK) response to the SIP BYE request interact with the media plane as specified in 3GPP TS 24.380 [5].

9 Affiliation

9.1 General

Subclause 9.2 contains the procedures for explicit affiliation at the MCPTT client, the MCPTT server serving the MCPTT user and the MCPTT server owning the MCPTT group.

Subclause 9.2 contains the procedures for implicit affiliation at the MCPTT server serving the MCPTT user and the MCPTT server owning the MCPTT group.

Subclause 9.3 describes the coding used for explicit affiliation.

The procedures for implicit affiliation in this clause are triggered at the MCPTT server serving the MCPTT user in the following circumstances:

- on receipt of a SIP INVITE request or a SIP REFER request from an MCPTT client to join an MCPTT chat group, where the MCPTT client is not already affiliated to the MCPTT group;

- on receipt of a SIP INVITE request or a SIP REFER request from an MCPTT client when attempting to initiate an MCPTT emergency group call or MCPTT imminent peril group call and the MCPTT client is not already affiliated to the MCPTT group;

- on receipt of a SIP MESSAGE request from an MCPTT client when initiating an MCPTT emergency alert targeted to an MCPTT group and the MCPTT client is not already affiliated to the MCPTT group; and

- on receipt of a SIP REGISTER request for service authorisation (as described in subclause 7.3.2) or SIP PUBLISH request for service authorisation and service settings (as described in subclause 7.3.2), as determined by configuration in the MCPTT user profile document as specified in 3GPP TS 24.484 [50].

The procedures for implicit affiliation in this clause are triggered at the MCPTT server owning the MCPTT group in the following circumstances:

- on receipt of a SIP INVITE request from the MCPTT server serving the MCPTT user where an MCPTT user wants to join an MCPTT chat group and the MCPTT client is not already affiliated to the MCPTT group;

- on receipt of a SIP INVITE request from the MCPTT server serving the MCPTT user where an MCPTT user initiates an MCPTT emergency group call or MCPTT imminent peril group call and the MCPTT client is not already affiliated to the MCPTT group; and

- on receipt of a SIP MESSAGE request from the MCPTT server serving the MCPTT user when the MCPTT user initiates an MCPTT emergency alert targeted to an MCPTT group and the MCPTT client is not already affiliated to the MCPTT group.

9.2 Procedures

9.2.1 MCPTT client procedures

9.2.1.1 General

The MCPTT client procedures consist of:

- an affiliation status change procedure;

- an affiliation status determination procedure;

- a procedure for sending affiliation status change request in negotiated mode to target MCPTT user; and

- a procedure for receiving affiliation status change request in negotiated mode from authorized MCPTT user.

In order to obtain information about success or rejection of changes triggered by the affiliation status change procedure for an MCPTT user, the MCPTT client needs to initiate the affiliation status determination procedure for the MCPTT user before starting the affiliation status change procedure for the MCPTT user.

9.2.1.2 Affiliation status change procedure

In order:

- to indicate that an MCPTT user is interested in one or more MCPTT group(s) at an MCPTT client;

- to indicate that the MCPTT user is no longer interested in one or more MCPTT group(s) at the MCPTT client;

- to refresh indication of an MCPTT user interest in one or more MCPTT group(s) at an MCPTT client due to near expiration of the expiration time of an MCPTT group with the affiliation status set to the "affiliated" state received in a SIP NOTIFY request in subclause 9.2.1.3;

- to send an affiliation status change request in mandatory mode to another MCPTT user; or

- any combination of the above;

the MCPTT client shall generate a SIP PUBLISH request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37], and IETF RFC 3856 [51].

In the SIP PUBLISH request, the MCPTT client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall include the <mcptt-request-uri> element set to the MCPTT ID of the MCPTT user;

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-Preferred-Service header field according to IETF RFC 6050 [9];

4) if the targeted MCPTT user is interested in at least one MCPTT group at the targeted MCPTT client, shall set the Expires header field according to IETF RFC 3903 [37], to 4294967295;

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

5) if the targeted MCPTT user is no longer interested in any MCPTT group at the targeted MCPTT client, shall set the Expires header field according to IETF RFC 3903 [37], to zero; and

6) shall include an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 9.3.1. In the MIME body, the MCPTT client:

   a) shall include all MCPTT groups where the targeted MCPTT user indicates its interest at the targeted MCPTT client;

   b) shall include the MCPTT client ID of the targeted MCPTT client;

   c) shall not include the "status" attribute and the "expires" attribute in the <affiliation> element; and

   d) shall set the <p-id> child element of the <presence> root element to a globally unique value.

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

9.2.1.3 Affiliation status determination procedure

NOTE 1: The MCPTT UE also uses this procedure to determine which MCPTT groups the MCPTT user successfully affiliated to.

In order to discover MCPTT groups:

1) which the MCPTT user at an MCPTT client is affiliated to; or

2) which another MCPTT user is affiliated to;

the MCPTT client shall generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26].

In the SIP SUBSCRIBE request, the MCPTT client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall include the <mcptt-request-uri> element set to the MCPTT ID of the targeted MCPTT user;

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-Preferred-Service header field according to IETF RFC 6050 [9];

4) if the MCPTT client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295;

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

5) if the MCPTT client wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [26], to zero; and

6) shall include an Accept header field containing the application/pidf+xml MIME type; and

7) if requesting MCPTT groups where the MCPTT user is affiliated to at the MCPTT client, shall include an application/simple-filter+xml MIME body indicating per-client restrictions of presence event package notification information according to subclause 9.3.2, indicating the MCPTT client ID of the MCPTT client.

In order to re-subscribe or de-subscribe, the MCPTT client shall generate an in-dialog SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26]. In the SIP SUBSCRIBE request, the MCPTT client:

1) if the MCPTT client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295;

NOTE 3: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

2) if the MCPTT client wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [26], to zero; and

3) shall include an Accept header field containing the application/pidf+xml MIME type.

Upon receiving a SIP NOTIFY request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26], if SIP NOTIFY request contains an application/pidf+xml MIME body indicating per-user affiliation information constructed according to subclause 9.3.1, then the MCPTT client shall determine affiliation status of the MCPTT user for each MCPTT group at the MCPTT client(s) in the MIME body. If the <p-id> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request is included, the <p-id> element value indicates the SIP PUBLISH request which triggered sending of the SIP NOTIFY request.

9.2.1.4 Procedure for sending affiliation status change request in negotiated mode to target MCPTT user

NOTE: Procedure for sending affiliation status change request in negotiated mode to several target MCPTT users is not supported in this version of the specification.

Upon receiving a request from the MCPTT user to send an affiliation status change request in negotiated mode to a target MCPTT user, the MCPTT client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33]. In the SIP MESSAGE request, the MCPTT client:

1) shall set the Request-URI to the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall include the <mcptt-request-uri> element set to the MCPTT ID of the target MCPTT user;

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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP MESSAGE request;

4) shall include an application/vnd.3gpp.mcptt-affiliation-command+xml MIME body as specified in Annex F.4; and

5) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP MESSAGE request, the MCPTT client shall indicate to the user that the request has been delivered to an MCPTT client of the target MCPTT user.

9.2.1.5 Procedure for receiving affiliation status change request in negotiated mode from authorized MCPTT user

Upon receiving a SIP MESSAGE request containing:

1) 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 header field according to IETF RFC 6050 [9]; and

2) an application/vnd.3gpp.mcptt-affiliation-command+xml MIME body with a list of MCPTT groups for affiliation under the <affiliate> element and a list of MCPTT groups for de-affiliation under the <de-affiliate> element;

then the MCPTT client:

1) shall send a 200 (OK) response to the SIP MESSAGE request;

2) shall seek confirmation of the list of MCPTT groups for affiliation and the list of MCPTT groups for de-affiliation, resulting in an accepted list of MCPTT groups for affiliation and an accepted list of MCPTT groups for de-affiliation; and

3) if the user accepts the request:

   a) shall perform affiliation for each entry in the accepted list of MCPTT groups for affiliation for which the MCPTT client is not affiliated, as specified in subclause 9.2.1.2; and

   b) shall perform de-affiliation for each entry in the accepted list of MCPTT groups for de-affiliation for which the MCPTT client is affiliated, as specified in subclause 9.2.1.2.

9.2.2 MCPTT server procedures

9.2.2.1 General

The MCPTT server procedures consist of:

- procedures of MCPTT server serving the MCPTT user; and
- procedures of MCPTT server owning the MCPTT group.

9.2.2.2 Procedures of MCPTT server serving the MCPTT user

9.2.2.2.1 General

The procedures of MCPTT server serving the MCPTT user consist of:

- a receiving affiliation status change from MCPTT client procedure;
- a receiving subscription to affiliation status procedure;
- a sending notification of change of affiliation status procedure;
- a sending affiliation status change towards MCPTT server owning MCPTT group procedure;
- an affiliation status determination from MCPTT server owning MCPTT group procedure;
- a procedure for authorizing affiliation status change request in negotiated mode sent to served MCPTT user;
- a forwarding affiliation status change towards another MCPTT user procedure;
- a forwarding subscription to affiliation status towards another MCPTT user procedure
- an affiliation status determination procedure;
- an affiliation status change by implicit affiliation procedure;

- an implicit affiliation status change completion procedure;
- an implicit affiliation status change cancellation procedure; and
- an implicit affiliation to configured groups procedure.

9.2.2.2.2 Stored information

The MCPTT server shall maintain a list of MCPTT user information entries. The list of the MCPTT user information entries contains one MCPTT user information entry for each served MCPTT ID.

In each MCPTT user information entry, the MCPTT server shall maintain:

1) an MCPTT ID. This field uniquely identifies the MCPTT user information entry in the list of the MCPTT user information entries; and
2) a list of MCPTT client information entries.

In each MCPTT client information entry, the MCPTT server shall maintain:

1) an MCPTT client ID. This field uniquely identifies the MCPTT client information entry in the list of the MCPTT client information entries; and
2) a list of MCPTT group information entries.

In each MCPTT group information, the MCPTT server shall maintain:

1) an MCPTT group ID. This field uniquely identifies the MCPTT group information entry in the list of the MCPTT group information entries;
2) an affiliation status;
3) an expiration time;
4) an affiliating p-id; and
5) a next publishing time.

9.2.2.2.3 Receiving affiliation status change from MCPTT client procedure

Upon receiving a SIP PUBLISH request such that:

1) Request-URI of the SIP PUBLISH request contains either the public service identity identifying the originating participating MCPTT function serving the MCPTT user, or the public service identity identifying the terminating participating MCPTT function serving the MCPTT user;
2) the SIP PUBLISH request contains an application/vnd.3gpp.mcptt-info+xml MIME body containing the<mcptt-request-uri> element which identifies an MCPTT ID served by the MCPTT server;
3) 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 header field according to IETF RFC 6050 [9];
4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and
5) SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 9.3.1;

then the MCPTT server:

1) shall identify the served MCPTT ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP PUBLISH request;
2) if the Request-URI of the SIP PUBLISH request contains the public service identity identifying the originating participating MCPTT function serving the MCPTT user, shall identify the originating MCPTT ID from public user identity in the P-Asserted-Identity header field of the SIP PUBLISH request;

3) if the Request-URI of the SIP PUBLISH request contains the public service identity identifying the terminating participating MCPTT function serving the MCPTT user, shall identify the originating MCPTT ID in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP PUBLISH request;

4) if the originating MCPTT ID is different than the served MCPTT ID and the originating MCPTT ID is not authorized to modify affiliation status of the served MCPTT ID, shall send a 403 (Forbidden) response and shall not continue with the rest of the steps;

5) if the Expires header field of the SIP PUBLISH request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP PUBLISH request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;

6) if the Expires header field of the SIP PUBLISH request has nonzero value, shall determine the candidate expiration interval to according to IETF RFC 3903 [37];

7) if the Expires header field of the SIP PUBLISH request has zero value, shall set the candidate expiration interval to zero;

8) shall respond with SIP 200 (OK) response to the SIP PUBLISH request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37]. In the SIP 200 (OK) response, the MCPTT server:

   a) shall set the Expires header field according to IETF RFC 3903 [37], to the candidate expiration time;

9) if the "entity" attribute of the <presence> element of the application/pidf+xml MIME body of the SIP PUBLISH request is different than the served MCPTT ID, shall not continue with the rest of the steps;

10) shall identify the served MCPTT client ID in the "id" attribute of the <tuple> element of the <presence> element of the application/pidf+xml MIME body of the SIP PUBLISH request;

11) shall consider an MCPTT user information entry such that:

   a) the MCPTT user information entry is in the list of MCPTT user information entries described in subclause 9.2.2.2.2; and

   b) the MCPTT ID of the MCPTT user information entry is equal to the served MCPTT ID;

   as the served MCPTT user information entry;

12) shall consider an MCPTT client information entry such that:

   a) the MCPTT client information entry is in the list of MCPTT client information entries of the served MCPTT user information entry; and

   b) the MCPTT client ID of the MCPTT client information entry is equal to the served MCPTT client ID;

   as the served MCPTT client information entry;

13) shall consider a copy of the list of the MCPTT group information entries of the served MCPTT client information entry as the served list of the MCPTT group information entries;

14) if the candidate expiration interval is nonzero:

   a) shall construct the candidate list of the MCPTT group information entries as follows:

      i) for each MCPTT group ID which has an MCPTT group information entry in the served list of the MCPTT group information entries, such that the expiration time of the MCPTT group information entry has not expired yet, and which is indicated in a "group" attribute of an <affiliation> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

         A) shall copy the MCPTT group information entry into a new MCPTT group information entry of the candidate list of the MCPTT group information entries;

B) if the affiliation status of the MCPTT group information entry is "deaffiliating" or "deaffiliated", shall set the affiliation status of the new MCPTT group information entry to the "affiliating" state and shall reset the affiliating p-id of the new MCPTT group information entry; and

C) shall set the expiration time of the new MCPTT group information entry to the current time increased with the candidate expiration interval;

ii) for each MCPTT group ID which has an MCPTT group information entry in the served list of the MCPTT group information entries, such that the expiration time of the MCPTT group information entry has not expired yet, and which is not indicated in any "group" attribute of the <affiliation> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

A) shall copy the MCPTT group information entry into a new MCPTT group information entry of the candidate list of the MCPTT group information entries; and

B) if the affiliation status of the MCPTT group information entry is "affiliated" or "affiliating":

- shall set the affiliation status of the new MCPTT group information entry to the "de-affiliating" state; and

- shall set the expiration time of the new MCPTT group information entry to the current time increased with twice the value of timer F; and

iii) for each MCPTT group ID:

A) which does not have an MCPTT group information entry in the served list of the MCPTT group information entries; or

B) which has an MCPTT group information entry in the served list of the MCPTT group information entries, such that the expiration time of the MCPTT group information entry has already expired;

and which is indicated in a "group" element of the <affiliation> element of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request:

A) shall add a new MCPTT group information entry in the candidate list of the MCPTT group information list for the MCPTT group ID;

B) shall set the affiliation status of the new MCPTT group information entry to the "affiliating" state;

C) shall set the expiration time of the new MCPTT group information entry to the current time increased with the candidate expiration interval; and

D) shall reset the affiliating p-id of the new MCPTT group information entry;

b) determine the candidate number of MCPTT group IDs as number of different MCPTT group IDs which have an MCPTT group information entry:

i) in the candidate list of the MCPTT group information entries; or

ii) in the list of the MCPTT group information entries of an MCPTT client information entry such that:

A) the MCPTT client information entry is in the list of the MCPTT client information entries of the served MCPTT user information entry; and

B) the MCPTT client ID of the MCPTT client information entry is not equal to the served MCPTT client ID;

with the affiliation status set to the "affiliating" state or the "affiliated" state and with the expiration time which has not expired yet; and

c) if the candidate number of MCPTT group IDs is bigger than N2 value of the served MCPTT ID, shall based on MCPTT service provider policy reduce the candidate MCPTT group IDs to that equal to N2;

NOTE: The MCPTT service provider policy can determine to remove an MCPTT group ID based on the order it appeared in the PUBLISH request or based on the importance or priority of the MCPTT group or some other policy to determine which MCPTT groups are preferred.

15) if the candidate expiration interval is zero, constructs the candidate list of the MCPTT group information entries as follows:

   a) for each MCPTT group ID which has an entry in the served list of the MCPTT group information entries:

      i) shall copy the MCPTT group entry of the served list of the MCPTT group information into a new MCPTT group information entry of the candidate list of the MCPTT group information entries;

      ii) shall set the affiliation status of the new MCPTT group information entry to the "de-affiliating" state; and

      iii) shall set the expiration time of the new MCPTT group information entry to the current time increased with twice the value of timer F;

16) shall replace the list of the MCPTT group information entries stored in the served MCPTT client information entry with the candidate list of the MCPTT group information entries;

17) shall perform the procedures specified in subclause 9.2.2.2.6 for the served MCPTT ID and each MCPTT group ID:

   a) which does not have an MCPTT group information entry in the served list of the MCPTT group information entries and which has an MCPTT group information entry in the candidate list of the MCPTT group information entries with the affiliation status set to the "affiliating" state;

   b) which has an MCPTT group information entry in the served list of the MCPTT group information entries with the expiration time already expired, and which has an MCPTT group information entry in the candidate list of the MCPTT group information entries with the affiliation status set to the "affiliating" state;

   c) which has an MCPTT group information entry in the served list of the MCPTT group information entries with the affiliation status set to the "deaffiliating" state or the "deaffiliated" state and with the expiration time not expired yet, and which has an MCPTT group information entry in the candidate list of the MCPTT group information entries with the affiliation status set to the "affiliating" state; or

   d) which has an MCPTT group information entry in the served list of the MCPTT group information entries with the affiliation status set to the "affiliated" state and with the expiration time not expired yet, and which has an MCPTT group information entry in the candidate list of the MCPTT group information entries with the affiliation status set to the "de-affiliating" state;

18) shall identify the handled p-id in the <p-id> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request; and

19) shall perform the procedures specified in subclause 9.2.2.2.5 for the served MCPTT ID.

9.2.2.2.4 Receiving subscription to affiliation status procedure

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains either the public service identity identifying the originating participating MCPTT function serving the MCPTT user, or the public service identity identifying the terminating participating MCPTT function serving the MCPTT user;

2) the SIP SUBSCRIBE request contains an application/vnd.3gpp.mcptt-info+xml MIME body containing the<mcptt-request-uri> element which identifies an MCPTT ID served by the MCPTT server;

3) 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 header field according to IETF RFC 6050 [9]; and

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type;

the MCPTT server:

1) shall identify the served MCPTT ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP SUBSCRIBE request;

2) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the originating participating MCPTT function serving the MCPTT user, shall identify the originating MCPTT ID from public user identity in the P-Asserted-Identity header field of the SIP SUBSCRIBE request;

3) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the terminating participating MCPTT function serving the MCPTT user, shall identify the originating MCPTT ID in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP SUBSCRIBE request;

4) if the originating MCPTT ID is different than the served MCPTT ID and the originating MCPTT ID is not authorized to modify affiliation status of the served MCPTT ID, shall send a 403 (Forbidden) response and shall not continue with the rest of the steps; and

5) shall generate a 200 (OK) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 6665 [26].

For the duration of the subscription, the MCPTT server shall notify the subscriber about changes of the information of the served MCPTT ID, as described in subclause 9.2.2.2.5.

9.2.2.2.5 Sending notification of change of affiliation status procedure

In order to notify the subscriber about changes of the served MCPTT ID, the MCPTT server:

1) shall consider an MCPTT user information entry such that:

   a) the MCPTT user information entry is in the list of MCPTT user information entries described in subclause 9.2.2.2.2; and

   b) the MCPTT ID of the MCPTT user information entry is equal to the served MCPTT ID;

   as the served MCPTT user information entry;

2) shall consider the list of the MCPTT client information entries of the served MCPTT user information entry as the served list of the MCPTT client information entries;

3) shall generate an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 9.3.1 and the served list of the MCPTT client information entries with the following clarifications:

   a) the MCPTT server shall not include information from an MCPTT group information entry with the expiration time already expired;

   b) the MCPTT server shall not include information from an MCPTT group information entry with the affiliation status set to the "deaffiliated" state;

   c) if the SIP SUBSCRIBE request creating the subscription of this notification contains an application/simple-filter+xml MIME body indicating per-client restrictions of presence event package notification information according to subclause 9.3.2, the MCPTT server shall restrict the application/pidf+xml MIME body according to the application/simple-filter+xml MIME body; and

   d) if this procedures is invoked by procedure in subclause 9.2.2.2.3 where the handled p-id value was identified, the MCPTT server shall set the <p-id> child element of the <presentity> root element of the application/pidf+xml MIME body of the SIP NOTIFY request to the handled p-id value; and

4) send a SIP NOTIFY request according to 3GPP TS 24.229 [4], and IETF RFC 6665 [26] for the subscription created in subclause 9.2.2.2.4. In the SIP NOTIFY request, the MCPTT server shall include the generated application/pidf+xml MIME body indicating per-user affiliation information.

9.2.2.2.6 Sending affiliation status change towards MCPTT server owning MCPTT group procedure

NOTE 1: Usage of one SIP PUBLISH request to carry information about change of affiliation state of several MCPTT users served by the same MCPTT server is not supported in this version of the specification.

In order:

- to send an affiliation request of a served MCPTT ID to a handled MCPTT group ID;
- to send an de-affiliation request of a served MCPTT ID from a handled MCPTT group ID; or
- to send an affiliation request of a served MCPTT ID to a handled MCPTT group ID due to near expiration of the previously published information;

the MCPTT server shall generate a SIP PUBLISH request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51]. In the SIP PUBLISH request, the MCPTT server:

1) shall set the Request-URI to the public service identity of the controlling MCPTT function associated with the handled MCPTT group ID;
2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT server:
   a) shall include the <mcptt-request-uri> element set to the handled MCPTT group ID; and
   b) shall include the <mcptt-calling-user-id> element set to the served MCPTT ID;
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 header field according to IETF RFC 6050 [9];
4) if sending an affiliation request, shall set the Expires header field according to IETF RFC 3903 [37], to 4294967295;

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

5) if sending an de-affiliation request, shall set the Expires header field according to IETF RFC 3903 [37], to zero;
6) shall include an P-Asserted-Identity header field set to the public service identity of the MCPTT server according to 3GPP TS 24.229 [4];
7) shall set the current p-id to a globally unique value;
8) shall consider an MCPTT user information entry such that:
   a) the MCPTT user information entry is in the list of MCPTT user information entries described in subclause 9.2.2.2.2; and
   b) the MCPTT ID of the MCPTT user information entry is equal to the served MCPTT ID;

   as the served MCPTT user information entry;
9) for each MCPTT group information entry such that:
   a) the MCPTT group information entry has the "affiliating" affiliation status, the MCPTT group ID set to the handled MCPTT group ID, the expiration time has not expired yet and the affiliating p-id is not set;
   b) the MCPTT group information entry is in the list of the MCPTT group information entries of an MCPTT client information entry; and
   c) the MCPTT client information entry is in the list of the MCPTT client information entries of the served MCPTT user information entry;

   shall set the affiliating p-id of the MCPTT group information entry to the current p-id; and
10) shall include an application/pidf+xml MIME body indicating per-group affiliation information constructed according to subclause 9.2.3.2. The MCPTT server shall indicate all served MCPTT client IDs, such that:
   a) the affiliation status is set to "affiliating" or "affiliated", and the expiration time has not expired yet in an MCPTT group information entry with the MCPTT group ID set to the handled MCPTT group;
   b) the MCPTT group information entry is in the list of the MCPTT group information entries of an MCPTT client information entry;

c) the MCPTT client information entry has the MCPTT client ID set to the served MCPTT client ID; and

d) the MCPTT client information entry is in the list of the MCPTT client information entries of the served MCPTT user information entry.

The MCPTT server shall set the <p-id> child element of the <presence> root element to the current p-id.

The MCPTT server shall not include the "expires" attribute in the <affiliation> element.

The MCPTT server shall send the SIP PUBLISH request according to 3GPP TS 24.229 [4].

If timer F expires for the SIP PUBLISH request sent for a (de)affiliation request of served MCPTT ID to the MCPTT group ID or upon receiving a SIP 3xx, 4xx, 5xx or 6xx response to the SIP PUBLISH request, the MCPTT server:

1) shall remove each MCPTT group ID entry such that:

   a) the MCPTT group information entry has the MCPTT group ID set to the handled MCPTT group ID;

   b) the MCPTT group information entry is in the list of the MCPTT group information entries of an MCPTT client information entry; and

   c) the MCPTT client information entry is in the list of the MCPTT client information entries of the served MCPTT user information entry.

9.2.2.2.7 Affiliation status determination from MCPTT server owning MCPTT group procedure

NOTE 1: Usage of one SIP SUBSCRIBE request to subscribe for notification about change of affiliation state of several MCPTT users served by the same MCPTT server is not supported in this version of the specification.

In order to discover whether a served MCPTT user was successfully affiliated to a handled MCPTT group in the MCPTT server owning the handled MCPTT group, the MCPTT server shall generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26].

In the SIP SUBSCRIBE request, the MCPTT server:

1) shall set the Request-URI to the public service identity of the controlling MCPTT function associated with the handled MCPTT group ID;

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT server:

   a) shall include the <mcptt-request-uri> element set to the handled MCPTT group ID; and

   b) shall include the <mcptt-calling-user-id> element set to the served MCPTT ID;

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 header field according to IETF RFC 6050 [9];

4) if the MCPTT server wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295;

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

5) if the MCPTT server wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [26], to zero;

6) shall include an Accept header field containing the application/pidf+xml MIME type; and

7) shall include an application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information according to subclause 9.3.2, indicating the served MCPTT ID.

In order to re-subscribe or de-subscribe, the MCPTT server shall generate an in-dialog SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26]. In the SIP SUBSCRIBE request, the MCPTT server:

1) if the MCPTT server wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295;

NOTE 3: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

2) if the MCPTT server wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [26], to zero; and

3) shall include an Accept header field containing the application/pidf+xml MIME type.

Upon receiving a SIP NOTIFY request according to 3GPP TS 24.229 [4], IETF RFC 3856 [51], and IETF RFC 6665 [26], if SIP NOTIFY request contains an application/pidf+xml MIME body indicating per-group affiliation information constructed according to subclause 9.3.1, then the MCPTT server:

1) for each served MCPTT ID and served MCPTT client ID such that the application/pidf+xml MIME body of SIP NOTIFY request contains:

   a) a <tuple> element of the root <presence> element;

   b) the "id" attribute of the <tuple> element indicating the served MCPTT ID;

   c) an <affiliation> child element of the <status> element of the <tuple> element;

   d) the "client" attribute of the <affiliation> element indicating the served MCPTT client ID; and

   d) the "expires" attribute of the <affiliation> element indicating expiration of affiliation;

   perform the following:

   a) if an MCPTT group information entry exists such that:

      i) the MCPTT group information entry has the "affiliating" affiliation status, the MCPTT group ID set to the handled MCPTT group ID, and the expiration time has not expired yet;

      ii) the MCPTT group information entry is in the list of the MCPTT group information entries of an MCPTT client information entry with the MCPTT client ID set to the served MCPTT client ID;

      iii) the MCPTT client information entry is in the list of the MCPTT client information entries of a served MCPTT user information entry with the MCPTT ID set to the served MCPTT ID; and

      iv) the MCPTT user information entry is in the list of MCPTT user information entries described in subclause 9.2.2.2.2; and

      shall set the affiliation status of the MCPTT group information entry to "affiliated"; and

      shall set the next publishing time of the MCPTT group information entry to the current time and half of the time between the current time and the expiration of affiliation; and

2) for each MCPTT group information entry such that:

   a) the MCPTT group information entry has the "affiliated" affiliation status or the "deaffiliating" affiliation status, the MCPTT group ID set to the handled MCPTT group ID, and the expiration time has not expired yet;

   b) the MCPTT group information entry is in the list of the MCPTT group information entries of an MCPTT client information entry with the MCPTT client ID set to a served MCPTT client ID;

   c) the MCPTT client information entry is in the list of the MCPTT client information entries of the served MCPTT user information entry with the MCPTT ID set to a served MCPTT ID; and

   d) the MCPTT user information entry is in the list of MCPTT user information entries described in subclause 9.2.2.2.2; and

for which the application/pidf+xml MIME body of SIP NOTIFY request does not contain:

a) a <tuple> element of the root <presence> element;

b) the "id" attribute of the <tuple> element indicating the served MCPTT ID;

c) an <affiliation> child element of the <status> child element of the <tuple> element; and

d) the "client" attribute of the <affiliation> element indicating the served MCPTT client ID.

perform the following:

a) shall set the affiliation status of the MCPTT group information entry to "deaffiliated"; and

b) shall set the expiration time of the MCPTT group information entry to the current time; and

3) if a <p-id> element is included in the <presence> root element of the application/pidf+xml MIME body of the SIP NOTIFY request, then for each MCPTT group information entry such that:

a) the MCPTT group information entry has the "affiliating" affiliation status, the MCPTT group ID set to the handled MCPTT group ID, the expiration time has not expired yet and with the affiliating p-id set to the value of the <p-id> element;

b) the MCPTT group information entry is in the list of the MCPTT group information entries of an MCPTT client information entry with the MCPTT client ID set to a served MCPTT client ID;

c) the MCPTT client information entry is in the list of the MCPTT client information entries of the served MCPTT user information entry with the MCPTT ID set to a served MCPTT ID; and

d) the MCPTT user information entry is in the list of MCPTT user information entries described in subclause 9.2.2.2.2; and

for which the application/pidf+xml MIME body of SIP NOTIFY request does not contain:

a) a <tuple> element of the root <presence> element;

b) the "id" attribute of the <tuple> element indicating the served MCPTT ID;

c) an <affiliation> child element of the <status> child element of the <tuple> element; and

d) the "client" attribute of the <affiliation> element indicating the served MCPTT client ID;

perform the following:

a) shall set the affiliation status of the MCPTT group information entry to "deaffiliated"; and

b) shall set the expiration time of the MCPTT group information entry to the current time.

9.2.2.2.8 Procedure for authorizing affiliation status change request in negotiated mode sent to served MCPTT user

Upon receiving a SIP MESSAGE request such that:

1) Request-URI of the SIP MESSAGE request contains the public service identity identifying the terminating participating MCPTT function serving the MCPTT user;

2) the SIP MESSAGE request contains an application/vnd.3gpp.mcptt-info+xml MIME body containing the<mcptt-request-uri> element and the <mcptt-calling-user-id> element;

3) 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 header field according to IETF RFC 6050 [9]; and

4) the SIP MESSAGE request contains an application/vnd.3gpp.mcptt-affiliation-command+xml MIME body;

then the MCPTT server:

1) shall identify the served MCPTT ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP MESSAGE request;

2) shall identify the originating MCPTT ID in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP MESSAGE request;

3) if the originating MCPTT ID is not authorized to send an affiliation status change request in negotiated mode to the served MCPTT ID, shall send a 403 (Forbidden) response and shall not continue with the rest of the steps;

4) shall set the Request-URI of the SIP MESSAGE request to the public user identity bound to the served MCPTT ID in the MCPTT server; and

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

before forwarding the SIP MESSAGE request further.

9.2.2.2.9 Forwarding affiliation status change towards another MCPTT user procedure

Upon receiving a SIP PUBLISH request such that:

1) Request-URI of the SIP PUBLISH request contains the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

2) the SIP PUBLISH request contains an application/vnd.3gpp.mcptt-info MIME body containing the<mcptt-request-uri> element which identifies an MCPTT ID not served by the MCPTT server;

3) 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 header field according to IETF RFC 6050 [9];

4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and

5) SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-user affiliation information according to subclause 9.3.1;

then the MCPTT server:

1) shall identify the target MCPTT ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info MIME body of the SIP PUBLISH request;

2) shall identify the originating MCPTT ID from public user identity in the P-Asserted-Identity header field of the SIP PUBLISH request;

3) shall generate a SIP PUBLISH request from the received SIP PUBLISH request. In the generated SIP PUBLISH request, the MCPTT server:

   a) shall set the Request-URI to the public service identity identifying the terminating participating MCPTT function serving the target MCPTT ID;

   b) shall include a P-Asserted-Identity header field containing the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

   c) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT server:

      A) shall include the <mcptt-request-uri> element set to the target MCPTT ID; and

      B) shall include the <mcptt-calling-user-id> element set to the originating MCPTT ID; and

   d) shall include other signalling elements from the received SIP PUBLISH request; and

4) shall send the generated SIP PUBLISH request according to 3GPP TS 24.229 [4].

The MCPTT server shall forward received SIP responses to the SIP PUBLISH request.

9.2.2.2.10 Forwarding subscription to affiliation status towards another MCPTT user procedure

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

2) the SIP SUBCRIBE request contains an application/vnd.3gpp.mcptt-info MIME body containing the<mcptt-request-uri> element which identifies an MCPTT ID not served by MCPTT server;

3) 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 header field according to IETF RFC 6050 [9]; and

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type;

then the MCPTT server:

1) shall identify the target MCPTT ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info MIME body of the SIP SUBSCRIBE request;

2) shall identify the originating MCPTT ID from public user identity in the P-Asserted-Identity header field of the SIP SUBSCRIBE request;

3) shall generate a SIP SUBSCRIBE request from the received SIP SUBSCRIBE request. In the generated SIP SUBSCRIBE request, the MCPTT server:

   a) shall set the Request-URI to the public service identity identifying the terminating participating MCPTT function serving the target MCPTT ID;

   b) shall include a P-Asserted-Identity header field containing the public service identity identifying the originating participating MCPTT function serving the MCPTT user;

   c) shall include an application/vnd.3gpp.mcptt-info+xml MIME body. In the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT server:

      A) shall include the <mcptt-request-uri> element set to the target MCPTT ID; and

      B) shall include the <mcptt-calling-user-id> element set to the originating MCPTT ID; and

   d) shall include other signalling elements from the received SIP SUBSCRIBE request; and

4) shall send the generated SIP SUBSCRIBE request according to 3GPP TS 24.229 [4].

The MCPTT server shall forward any received SIP responses to the SIP SUBSCRIBE request, any received SIP NOTIFY request and any received SIP responses to the SIP NOTIFY request.

9.2.2.2.11 Affiliation status determination

This subclause is referenced from other procedures.

If the participating MCPTT function needs to determine the affiliation status of an MCPTT user to an MCPTT group, the participating function:

1) shall find the user information entry in the list of MCPTT user information entries described in subclause 9.2.2.2.2 such that the MCPTT ID of the MCPTT user information entry is equal to the MCPTT ID of the originator of the received SIP request;

   a) if the applicable MCPTT group information entry cannot be found, then the participating MCPTT function shall determine that the MCPTT user is not affiliated to the MCPTT group at the MCPTT client and the skip the rest of the steps;

2) shall find the MCPTT client information entry in the list of MCPTT client information entries of MCPTT user information entry found in step 1) in which the MCPTT client id matches the value of the <mcptt-client-id> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP request;

a) if the applicable MCPTT client information entry cannot be found, then the participating MCPTT function shall determine that the MCPTT user is not affiliated to the MCPTT group at the MCPTT client and the skip the rest of the steps;

3) shall find the MCPTT group information entry in the list of MCPTT group information entries of MCPTT client information entry found in step 2 such that the MCPTT group identity matches the value of the identity of the targeted MCPTT group;

a) if the applicable MCPTT group information entry was found in step 3) and the affiliation status of the MCPTT group information entry is "affiliating" or "affiliated", shall determine that the MCPTT user at the MCPTT client to be affiliated to the targeted MCPTT group and skip the rest of the steps;

b) if the applicable MCPTT group information entry was found in step 3) and the affiliation status of the MCPTT group information entry is "deaffiliating" or "deaffiliated", shall determine that the MCPTT user at the MCPTT client to not be affiliated to the targeted MCPTT group and skip the rest of the steps; or

c) if the applicable MCPTT group information entry was not found in step 3), shall determine that the MCPTT user at the MCPTT client is not affiliated to the targeted MCPTT group.

9.2.2.2.12 Affiliation status change by implicit affiliation

This subclause is referenced from other procedures.

Upon receiving a SIP request that requires implicit affiliation of the sending MCPTT client to an MCPTT group, the participating MCPTT function:

1) shall determine the served MCPTT client ID from the <mcptt-client-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP request;

2) shall determine the MCPTT group ID from the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP request;

3) shall determine the served MCPTT ID by using the public user identity in the P-Asserted-Identity header field of the SIP request;

NOTE 1: 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.

4) shall consider an MCPTT user information entry such that:

a) the MCPTT user information entry is in the list of MCPTT user information entries described in subclause 9.2.2.2.2; and

b) the MCPTT ID of the MCPTT user information entry is equal to the served MCPTT ID;

as the served MCPTT user information entry;

5) shall consider an MCPTT client information entry such that:

a) the MCPTT client information entry is in the list of MCPTT client information entries of the served MCPTT user information entry; and

b) the MCPTT client ID of the MCPTT client information entry is equal to the served MCPTT client ID;

as the served MCPTT client information entry;

6) shall consider a copy of the list of the MCPTT group information entries of the served MCPTT client information entry as the served list of the MCPTT group information entries;

7) shall construct the candidate list of the MCPTT group information entries as follows:

a) for each MCPTT group ID which has an MCPTT group information entry in the served list of the MCPTT group information entries shall copy the MCPTT group information entry into a new MCPTT group information entry of the candidate list of the MCPTT group information entries; and

b) if the determined MCPTT group ID does not have an MCPTT group information entry in the served list of the MCPTT group information entries or has an MCPTT group information entry in the served list of the MCPTT group information entries, such that the expiration time of the MCPTT group information entry has already expired:

i) shall add a new MCPTT group information entry in the candidate list of the MCPTT group information list for the determined MCPTT group ID;

ii) shall set the affiliation status of the new MCPTT group information entry to the "affiliating" state; and

iii) shall set the expiration time of the new MCPTT group information entry to the current time increased with the candidate expiration interval;

8) determine the candidate number of MCPTT group IDs as the number of different MCPTT group IDs which have an MCPTT group information entry:

a) in the candidate list of the MCPTT group information entries; or

b) in the list of the MCPTT group information entries of an MCPTT client information entry such that:

i) the MCPTT client information entry is in the list of the MCPTT client information entries of the served MCPTT user information entry; and

ii) the MCPTT client ID of the MCPTT client information entry is not equal to the served MCPTT client ID;

with the affiliation status set to the "affiliating" state or the "affiliated" state and with the expiration time which has not expired yet; and

9) if the candidate number of MCPTT group IDs is bigger than the N2 value of the served MCPTT ID, shall based on MCPTT service provider policy reduce the candidate MCPTT group IDs to that equal to N2;

NOTE 2: The MCPTT service provider policy can determine to remove an MCPTT group ID based on the importance or priority of other MCPTT groups, received SIP requests containing an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1 or other policy to determine which MCPTT groups are preferred.

10) if the determined MCPTT group ID cannot be added to the the candidate list of the MCPTT group information entries due to exceeding the MCPTT user's N2 limit, shall discard the candidate list of the MCPTT group information entries and skip the remaining steps of the current procedure; and

11) shall replace the list of the MCPTT group information entries stored in the served MCPTT client information entry with the candidate list of the MCPTT group information entries.

9.2.2.2.13 Implicit affiliation status change completion

This subclause is referenced from other procedures.

If the participating MCPTT function has received a SIP 2xx response from the controlling MCPTT function to a SIP request that had triggered performing the procedures of subclause 9.2.2.2.12, the participating MCPTT function:

1) shall set the affiliation status of the MCPTT group information entry added to the candidate list of the MCPTT group information entries by the procedures of subclause 9.2.2.2.12 to "affiliated"; and

2) shall perform the procedures specified in subclause 9.2.2.2.5 for the served MCPTT ID.

9.2.2.2.14 Implicit affiliation status change cancellation

This subclause is referenced from other procedures.

If the participating MCPTT function determines that a received SIP request that had triggered performing the procedures of subclause 9.2.2.2.12 needs to be rejected or if the participating MCPTT function receives a SIP 4xx, 5xx or 6xx response from the controlling MCPTT function for the received SIP request, the participating MCPTT function:

1) shall remove the MCPTT group ID entry added by the procedures of subclause 9.2.2.2.12 such that:

a) the MCPTT group information entry has the MCPTT group ID set to the MCPTT group ID of the MCPTT group targeted by the received SIP request;

b) the MCPTT group information entry is in the list of the MCPTT group information entries of an MCPTT client information entry containing the MCPTT client ID included in the received SIP request; and

c) the MCPTT client information entry is in the list of the MCPTT client information entries of the MCPTT user information entry containing the MCPTT ID of the sender of the received SIP request.

9.2.2.2.15 Implicit affiliation to configured groups procedure

This subclause is referenced from other procedures.

If the participating MCPTT function has successfully performed service authorization for the MCPTT ID identified in the service authorisation procedure as described in 3GPP TS 33.180 [78], the participating MCPTT function:

1) shall identify the MCPTT ID included in the SIP request received for service authorisation procedure as the served MCPTT ID;

2) shall identify the MCPTT client ID from the <mcptt-client-id> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body included in the SIP request received for service authorisation as the served MCPTT client ID;

3) 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 participating MCPTT function;

4) if no <ImplicitAffiliations> element is contained in the <OnNetwork> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) for the served MCPTT ID or the <ImplicitAffiliations> element contains no <entry> elements containing an MCPTT group ID, shall skip the remaining steps;

5) shall consider an MCPTT user information entry such that:

   a) the MCPTT user information entry is in the list of MCPTT user information entries described in subclause 9.2.2.2.2; and

   b) the MCPTT ID of the MCPTT user information entry is equal to the served MCPTT ID;

   as the served MCPTT user information entry;

6) shall consider an MCPTT client information entry such that:

   a) the MCPTT client information entry is in the list of MCPTT client information entries of the served MCPTT user information entry; and

   b) the MCPTT client ID of the MCPTT client information entry is equal to the served MCPTT client ID;

   as the served MCPTT client information entry;

7) shall consider a copy of the list of the MCPTT group information entries of the served MCPTT client information entry as the served list of the MCPTT group information entries;

8) shall construct the candidate list of the MCPTT group information entries as follows:

   a) for each MCPTT group ID which has an MCPTT group information entry in the served list of the MCPTT group information entries shall copy the MCPTT group information entry into a new MCPTT group information entry of the candidate list of the MCPTT group information entries;

   b) for each MCPTT group ID contained in an <entry> element of the <ImplicitAffiliations> element in the <OnNetwork> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) for the served MCPTT ID that does not have an MCPTT group information entry in the served list of the MCPTT group information entries or has an MCPTT group information entry in the served list of the MCPTT group information entries such that the expiration time of the MCPTT group information entry has already expired:

i) shall add a new MCPTT group information entry in the candidate list of the MCPTT group information list for the MCPTT group ID;

ii) shall set the affiliation status of the new MCPTT group information entry to the "affiliating" state; and

iii) shall set the expiration time of the new MCPTT group information entry to the current time increased with the candidate expiration interval;

c) if in step b) above, no new MCPTT group information entries were added to the candidate list of the MCPTT group information list for the MCPTT group ID:

i) shall discard the candidate list; and

ii) shall skip the remaining steps;

9) determine the candidate number of MCPTT group IDs as the number of different MCPTT group IDs which have an MCPTT group information entry:

a) in the candidate list of the MCPTT group information entries; or

b) in the list of the MCPTT group information entries of an MCPTT client information entry such that:

i) the MCPTT client information entry is in the list of the MCPTT client information entries of the served MCPTT user information entry; and

ii) the MCPTT client ID of the MCPTT client information entry is not equal to the served MCPTT client ID;

with the affiliation status set to the "affiliating" state or the "affiliated" state and with the expiration time which has not expired yet; and

c) if the candidate number of MCPTT group IDs is bigger than the N2 value of the served MCPTT ID, shall based on MCPTT service provider policy reduce the candidate MCPTT group IDs to that equal to N2;

NOTE 1: The MCPTT service provider policy can determine to remove an MCPTT group ID based on the importance or priority of other MCPTT groups, received SIP requests containing an authorised request for originating a priority call as determined by subclause 6.3.2.1.8.1 or other policy to determine which MCPTT groups are preferred.

10) shall replace the list of the MCPTT group information entries stored in the served MCPTT client information entry with the candidate list of the MCPTT group information entries; and

11) for each MCPTT group ID contained in an <entry> element of the <ImplicitAffiliations> element in the <OnNetwork> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) for the served MCPTT ID and which has an MCPTT group information entry in the candidate list of the MCPTT group information entries with an affiliation status of "affiliating", shall perform the procedures specified in subclause 9.2.2.2.6 for the served MCPTT ID and each MCPTT group ID.

NOTE 2: To learn of the MCPTT groups successfully affiliated to, the MCPTT client can subscribe to that information by the procedures specified in subclause 9.2.1.3.

9.2.2.3 Procedures of MCPTT server owning the MCPTT group

9.2.2.3.1 General

The procedures of MCPTT server owning the MCPTT group consist of:

- receiving group affiliation status change procedure;
- receiving subscription to affiliation status procedure;
- sending notification of change of affiliation status procedure;
- affiliation eligibility check procedure;
- implicit affiliation eligibility check procedure; and

- affiliation status change by implicit affiliation procedure.

NOTE: Usage of CSC-3 part of MCPTT group affiliation procedure and of CSC-3 part of MCPTT group de-affiliation procedure is not specified in this version of the specification.

9.2.2.3.2 Stored information

The MCPTT server shall maintain a list of MCPTT group information entries.

In each MCPTT group information entry, the MCPTT server shall maintain:

1) an MCPTT group ID. This field uniquely identifies the MCPTT group information entry in the list of the MCPTT group information entries; and

2) a list of MCPTT user information entries.

In each MCPTT user information entry, the MCPTT server shall maintain:

1) an MCPTT ID. This field uniquely identifies the MCPTT user information entry in the list of the MCPTT user information entries;

2) a list of MCPTT client information entries; and

3) an expiration time.

In each MCPTT client information entry, the MCPTT server shall maintain:

1) an MCPTT client ID. This field uniquely identifies the MCPTT client information entry in the list of the MCPTT client information entries.

9.2.2.3.3 Receiving group affiliation status change procedure

Upon receiving a SIP PUBLISH request such that:

1) Request-URI of the SIP PUBLISH request contains the public service identity of the controlling MCPTT function associated with the served MCPTT group;

2) the SIP PUBLISH request contains an application/vnd.3gpp.mcptt-info+xml MIME body containing the <mcptt-request-uri> element and the <mcptt-calling-user-id> element;

3) 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 header field according to IETF RFC 6050 [9];

4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and

5) SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-group affiliation information constructed according to subclause 9.2.3.2;

then the MCPTT server:

1) shall identify the served MCPTT group ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP PUBLISH request;

2) shall identify the handled MCPTT ID in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP PUBLISH request;

3) if the Expires header field of the SIP PUBLISH request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP PUBLISH request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;

4) if an MCPTT group for the served MCPTT group ID does not exist in the group management server according to 3GPP TS 24.481 [31], shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51] and skip the rest of the steps;

5) if the handled MCPTT ID is not a member of the MCPTT group identified by the served MCPTT group ID, shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51] and skip the rest of the steps;

6) shall respond with SIP 200 (OK) response to the SIP PUBLISH request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37]. In the SIP 200 (OK) response, the MCPTT server:

   a) shall set the Expires header field according to IETF RFC 3903 [37], to the selected expiration time;

7) if the "entity" attribute of the <presence> element of the application/pidf+xml MIME body of the SIP PUBLISH request is different than the served MCPTT group ID, shall not continue with the rest of the steps;

8) if the handled MCPTT ID is different from the MCPTT ID in the "id" attribute of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request, shall not continue with the rest of the steps;

9) shall consider an MCPTT group information entry such that:

   a) the MCPTT group information entry is in the list of MCPTT group information entries described in subclause 9.2.2.3.2; and

   b) the MCPTT group ID of the MCPTT group information entry is equal to the served MCPTT group ID;

   as the served MCPTT group information entry;

10) if the selected expiration time is zero:

   a) shall remove the MCPTT user information entry such that:

      i) the MCPTT user information entry is in the list of the MCPTT user information entries of the served MCPTT group information entry; and

      ii) the MCPTT user information entry has the MCPTT ID set to the served MCPTT ID;

11) if the selected expiration time is not zero:

   a) shall consider an MCPTT user information entry such that:

      i) the MCPTT user information entry is in the list of the MCPTT user information entries of the served MCPTT group information entry; and

      ii) the MCPTT ID of the MCPTT user information entry is equal to the handled MCPTT ID;

      as the served MCPTT user information entry;

   b) if the MCPTT user information entry does not exist:

      i) shall insert an MCPTT user information entry with the MCPTT ID set to the handled MCPTT ID into the list of the MCPTT user information entries of the served MCPTT group information entry; and

      ii) shall consider the inserted MCPTT user information entry as the served MCPTT user information entry; and

   c) shall set the following information in the served MCPTT user information entry:

      i) set the MCPTT client ID list according to the "client" attributes of the <affiliation> elements of the <status> element of the <tuple> element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request; and

      ii) set the expiration time according to the selected expiration time;

12) shall identify the handled p-id in the <p-id> child element of the <presence> root element of the application/pidf+xml MIME body of the SIP PUBLISH request; and

13) shall perform the procedures specified in subclause 9.2.2.3.5 for the served MCPTT group ID.

9.2.2.3.4 Receiving subscription to affiliation status procedure

NOTE: Usage of one SIP SUBSCRIBE request to subscribe for notification about change of affiliation state of several MCPTT users served by the same MCPTT server is not supported in this version of the specification.

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains the public service identity of the controlling MCPTT function associated with the served MCPTT group;

2) the SIP SUBSCRIBE request contains an application/vnd.3gpp.mcptt-info+xml MIME body containing the<mcptt-request-uri> element and the <mcptt-calling-user-id> element;

3) 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 header field according to IETF RFC 6050 [9];

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type; and

5) the SIP SUBSCRIBE request contains an application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information according to subclause 9.3.2 indicating the same MCPTT ID as in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP SUBSCRIBE request;

then the MCPTT server:

1) shall identify the served MCPTT group ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP SUBSCRIBE request;

2) shall identify the handled MCPTT ID in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP SUBSCRIBE request;

3) if the Expires header field of the SIP SUBSCRIBE request is not included or has nonzero value lower than 4294967295, shall send a SIP 423 (Interval Too Brief) response to the SIP SUBSCRIBE request, where the SIP 423 (Interval Too Brief) response contains a Min-Expires header field set to 4294967295, and shall not continue with the rest of the steps;

4) if an MCPTT group for the served MCPTT group ID does not exist in the group management server according to 3GPP TS 24.481 [31], shall reject the SIP SUBSCRIBE request with SIP 403 (Forbidden) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51] and skip the rest of the steps;

5) if the handled MCPTT ID is not a member of the MCPTT group identified by the served MCPTT group ID, shall reject the SIP SUBSCRIBE request with SIP 403 (Forbidden) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 3903 [37] and IETF RFC 3856 [51] and skip the rest of the steps; and

6) shall generate a SIP 200 (OK) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [4], IETF RFC 6665 [26].

For the duration of the subscription, the MCPTT server shall notify subscriber about changes of the information of the served MCPTT ID, as described in subclause 9.2.2.3.5.

9.2.2.3.5 Sending notification of change of affiliation status procedure

In order to notify the subscriber identified by the handled MCPTT ID about changes of the affiliation status of the served MCPTT group ID, the MCPTT server:

1) shall consider an MCPTT group information entry such that:

   a) the MCPTT group information entry is in the list of MCPTT group information entries described in subclause 9.2.2.3.2; and

   b) the MCPTT group ID of the MCPTT group information entry is equal to the served MCPTT group ID;

2) shall consider an MCPTT user information entry such:

   a) the MCPTT user information entry is in the list of the MCPTT user information entries of the served MCPTT group information entry; and

   b) the MCPTT ID of the MCPTT user information entry is equal to the handled MCPTT ID;

   as the served MCPTT user information entry;

3) shall generate an application/pidf+xml MIME body indicating per-group affiliation information according to subclause 9.3.1 and the served list of the served MCPTT user information entry of the MCPTT group information entry with following clarifications:

   a) the MCPTT server shall include the "expires" attribute in the <affiliation> element; and

   b) if this procedures is invoked by procedure in subclause 9.2.2.3.3 where the handled p-id was identified, the MCPTT server shall set the <p-id> child element of the <presentity> root element of the application/pidf+xml MIME body of the SIP NOTIFY request to the handled p-id value; and

4) send a SIP NOTIFY request according to 3GPP TS 24.229 [4], and IETF RFC 6665 [26] for the subscription created in subclause 9.2.2.3.4. In the SIP NOTIFY request, the MCPTT server shall include the generated application/pidf+xml MIME body indicating per-group affiliation information.

9.2.2.3.6 Implicit affiliation eligibility check procedure

This subclause is referenced from other procedures.

Upon receiving a SIP request for an MCPTT group that the MCPTT user is not currently affiliated to and that requires the controlling MCPTT function to check on the eligibility of the MCPTT user to be implicitly affiliated to the MCPTT group, the controlling MCPTT function:

1) shall perform the procedures of subclause 9.2.2.3.8 to determine if the MCPTT user is eligible to be affiliated to the MCPTT group; and

2) if the MCPTT user was determined eligible to be affiliated to the MCPTT group by the procedures of subclause 9.2.2.3.8, shall consider the MCPTT user to be eligible for implicit affiliation to the MCPTT group.

9.2.2.3.7 Affiliation status change by implicit affiliation procedure

This subclause is referenced from other procedures.

Upon receiving a SIP request for an MCPTT group that the MCPTT user is not currently affiliated to and that requires the controlling MCPTT function to perform an implicit affiliation to, the controlling MCPTT function:

1) shall identify the served MCPTT group ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP request;

2) shall identify the handled MCPTT ID in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP request;

3) shall consider an MCPTT group information entry such that:

   a) the MCPTT group information entry is in the list of MCPTT group information entries described in subclause 9.2.2.3.2; and

   b) the MCPTT group ID of the MCPTT group information entry is equal to the served MCPTT group ID;

   as the served MCPTT group information entry;

4) shall consider an MCPTT user information entry such that:

   a) the MCPTT user information entry is in the list of the MCPTT user information entries of the served MCPTT group information entry; and

   b) the MCPTT ID of the MCPTT user information entry is equal to the handled MCPTT ID;

as the served MCPTT user information entry;

c) if the MCPTT user information entry does not exist:

i) shall insert an MCPTT user information entry with the MCPTT ID set to the handled MCPTT ID into the list of the MCPTT user information entries of the served MCPTT group information entry; and

ii) shall consider the inserted MCPTT user information entry as the served MCPTT user information entry; and

d) shall make the following modifications in the served MCPTT user information entry:

i) add the MCPTT client ID derived from the received SIP request to the MCPTT client ID list if not already present; and

ii) set the expiration time as determined by local policy;

5) shall perform the procedures specified in subclause 9.2.2.3.5 for the served MCPTT group ID.

9.2.2.3.8 Affiliation eligibility check procedure

This subclause is referenced from other procedures.

Upon receiving a SIP request for an MCPTT group that the MCPTT user is not currently affiliated to and that requires the controlling MCPTT function to check on the eligibility of the MCPTT user to be affiliated to the MCPTT group, the controlling MCPTT function shall:

1) shall identify the served MCPTT group ID in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP request;

2) shall identify the handled MCPTT ID in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP request;

3) if an MCPTT group for the served MCPTT group ID does not exist in the group management server according to 3GPP TS 24.481 [31], shall consider the MCPTT user to be ineligible for affiliation and skip the rest of the steps;

4) if the handled MCPTT ID is not a member of the MCPTT group identified by the served MCPTT group ID, shall consider the MCPTT user to be ineligible for affiliation and skip the rest of the steps;

5) if there is no MCPTT group information entry in the list of MCPTT group information entries described in subclause 9.2.2.3.2 with an MCPTT group identity matching the served MCPTT group ID, then shall consider the MCPTT user to be ineligible for affiliation and skip the rest of the steps; or

6) shall consider the MCPTT user to be eligible for affiliation.

9.3 Coding

9.3.1 Extension of application/pidf+xml MIME type

9.3.1.1 Introduction

The subclauses of the parent subclause describe an extension of the application/pidf+xml MIME body specified in IETF RFC 3863 [52]. The extension is used to indicate:

- per-user affiliation information; and
- per-group affiliation information.

9.3.1.2 Syntax

The application/pidf+xml MIME body indicating per-user affiliation information is constructed according to IETF RFC 3863 [52] and:

1) contains a <presence> root element according to IETF RFC 3863 [52];
2) contains an "entity" attribute of the <presence> element set to the MCPTT ID of the MCPTT user;
3) contains one <tuple> child element according to IETF RFC 3863 [52] per each MCPTT client of the <presence> element;
4) can contain a <p-id> child element defined in the XML schema defined in table 9.3.1.2-1, of the <presence> element set to an identifier of a SIP PUBLISH request;
5) contains an "id" attribute of the <tuple> element set to the MCPTT client ID;
6) contains one <status> child element of each <tuple> element;
7) contains one <affiliation> child element defined in the XML schema defined in table 9.3.1.2-1, of the <status> element, for each MCPTT group in which the MCPTT user is interested at the MCPTT client;
8) contains a "group" attribute of each <affiliation> element set to the MCPTT group ID of the MCPTT group in which the MCPTT user is interested at the MCPTT client;
9) can contain a "status" attribute of each <affiliation> element indicating the affiliation status of the MCPTT user to MCPTT group at the MCPTT client; and
10) can contain an "expires" attribute of each <affiliation> element indicating expiration of affiliation of the MCPTT user to MCPTT group at the MCPTT client.

The application/pidf+xml MIME body indicating per-group affiliation information is constructed according to IETF RFC 3856 [51] and:

1) contains the <presence> root element according to IETF RFC 3863 [52];
2) contains an "entity" attribute of the <presence> element set to the MCPTT group ID of the MCPTT group;
3) contains one <tuple> child element according to IETF RFC 3863 [52] of the <presence> element;
4) can contain a <p-id> child element defined in the XML schema defined in table 9.3.1.2-1, of the <presence> element set to an identifier of a SIP PUBLISH request;
5) contains an "id" attribute of the <tuple> element set to the MCPTT ID of the MCPTT user;
6) contains one <status> child element of each <tuple> element;
7) contains one <affiliation> child element defined in the XML schema defined in table 9.3.1.2-1, of the <status> element, for each MCPTT client at which the MCPTT user is interested in the MCPTT group;
8) contains one "client" attribute defined in the XML schema defined in table 9.3.1.2-2, of the <affiliation> element set to the MCPTT client ID; and
9) can contain an "expires" attribute defined in the XML schema defined in table 9.3.1.2-2, of the <affiliation> element indicating expiration of affiliation of the MCPTT user to MCPTT group at the MCPTT client.

Table 9.3.1.2-1: XML schema with elements and attributes extending the application/pidf+xml MIME body

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:3gpp:ns:mcpttPresInfo:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:mcpttPI10="urn:3gpp:ns:mcpttPresInfo:1.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <!-- MCPTT specific child elements of tuple element -->
  <xs:element name="affiliation" type="mcpttPI10:affiliationType"/>
```

```
  <xs:complexType name="affiliationType">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="group" type="xs:anyURI" use="optional"/>
    <xs:attribute name="client" type="xs:anyURI" use="optional"/>
    <xs:attribute name="status" type="mcpttPI10:statusType" use="optional"/>
    <xs:attribute name="expires" type="xs:dateTime" use="optional"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:simpleType name="statusType">
    <xs:restriction base="xs:string">
      <xs:enumeration value="affiliating"/>
      <xs:enumeration value="affiliated"/>
      <xs:enumeration value="deaffiliating"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:element name="p-id" type="xs:string"/>

  </xs:schema>
```

The application/pidf+xml MIME body refers to namespaces using prefixes specified in table 9.3.1.2-2.

Table 9.3.1.2-2: Assignment of prefixes to namespace names in the application/pidf+xml MIME body

Prefix	Namespace
mcpttPI10	urn:3gpp:ns:mcpttPresInfo:1.0
NOTE: The "urn:ietf:params:xml:ns:pidf" namespace is the default namespace so no prefix is used for it in the application/pidf+xml MIME body.	

9.3.2 Extension of application/simple-filter+xml MIME type

9.3.2.1 Introduction

The subclauses of the parent subclause describe an extension of the application/simple-filter+xml MIME body specified in IETF RFC 4661 [63].

The extension is used to indicate per-client restrictions of presence event package notification information and per-user restrictions of presence event package notification information.

9.3.2.2 Syntax

The application/simple-filter+xml MIME body indicating per-client restrictions of presence event package notification information is constructed according to IETF RFC 4661 [63] and:

1) contains a <filter-set> root element according to IETF RFC 4661 [63];

2) contains a <ns-bindings> child element according to IETF RFC 4661 [63], of the <filter-set> element;

3) contains a <ns-binding> child element according to IETF RFC 4661 [63], of the <ns-bindings> element where the <ns-binding> element:

   A) does not contain a "prefix" attribute according to IETF RFC 4661 [63]; and

   B) contains an "urn" attribute set to the "urn:ietf:params:xml:ns:pidf" value;

4) contains a <ns-binding> child element according to IETF RFC 4661 [63], of the <ns-bindings> element where the <ns-binding> element:

   A) contains a "prefix" attribute according to IETF RFC 4661 [63], set to "mcpttPI10"; and

   B) contains an "urn" attribute according to IETF RFC 4661 [63], set to the "urn:3gpp:ns:mcpttPresInfo:1.0" value;

5) contains a <filter> child element according to IETF RFC 4661 [63], of the <filter-set> element where the <filter> element;

   A) contains an "id" attribute set to a value constructed according to IETF RFC 4661 [63];

   B) does not contain an "uri" attribute of the <filter> child element according to IETF RFC 4661 [63]; and

   C) does not contain an "domain" attribute according to IETF RFC 4661 [63];

6) contains a <what> child element according to IETF RFC 4661 [63], of the <filter> element; and

7) contains an <include> child element according to IETF RFC 4661 [63], of the <what> element where the <include> element;

   A) does not contain a "type" attribute according to IETF RFC 4661 [63]; and

   B) contains the value, according to IETF RFC 4661 [63], set to concatenation of the '//presence/tuple[@id="' string, the MCPTT client ID, and the '"]' string.

The application/simple-filter+xml MIME body indicating per-user restrictions of presence event package notification information is constructed according to IETF RFC 4661 [63] and:

1) contains a <filter-set> root element according to IETF RFC 4661 [63];

2) contains a <ns-bindings> child element according to IETF RFC 4661 [63], of the <filter-set> element;

3) contains a <ns-binding> child element according to IETF RFC 4661 [63], of the <ns-bindings> element where the <ns-binding> element:

   A) does not contain a "prefix" attribute according to IETF RFC 4661 [63]; and

   B) contains an "urn" attribute set to the "urn:ietf:params:xml:ns:pidf" value;

4) contains a <ns-binding> child element according to IETF RFC 4661 [63], of the <ns-bindings> element where the <ns-binding> element:

   A) contains a "prefix" attribute according to IETF RFC 4661 [63], set to "mcpttPI10"; and

   B) contains an "urn" attribute according to IETF RFC 4661 [63], set to the "urn:3gpp:ns:mcpttPresInfo:1.0" value;

5) contains a <filter> child element according to IETF RFC 4661 [63], of the <filter-set> element where the <filter> element;

   A) contains an "id" attribute set to a value constructed according to IETF RFC 4661 [63];

   B) does not contain an "uri" attribute of the <filter> child element according to IETF RFC 4661 [63]; and

   C) does not contain an "domain" attribute according to IETF RFC 4661 [63];

6) contains a <what> child element according to IETF RFC 4661 [63], of the <filter> element; and

7) contains an <include> child element according to IETF RFC 4661 [63], of the <what> element where the <include> element;

   A) does not contain a "type" attribute according to IETF RFC 4661 [63]; and

   B) contains the value, according to IETF RFC 4661 [63], set to concatenation of the '//presence/tuple[@id="' string, the MCPTT ID, and the '"]' string.

10 Group call

10.0 General

This subclause describes the group call procedures for on-network and off-network.

For on-network, prearranged group call including emergency group call for each functional entity are specified in subclause 10.1.1 and chat group (restricted) call including emergency group call for each functional entity are specified in subclause 10.1.2.

Off-network group call and off-network broadcast group call are specified in subclause 10.2 and subclause 10.3.

10.1 On-network group call

10.1.1 Prearranged group call

10.1.1.1 General

10.1.1.2 MCPTT client procedures

10.1.1.2.1 On-demand prearranged group call

10.1.1.2.1.1 Client originating procedures

Upon receiving a request from an MCPTT user to establish an MCPTT prearranged group session the MCPTT client shall generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) if the MCPTT user has requested the origination of an MCPTT emergency group call or is originating an MCPTT prearranged group call and the MCPTT emergency state is already set, the MCPTT client shall comply with the procedures in subclause 6.2.8.1.1;

2) if the MCPTT user has requested the origination of an MCPTT imminent peril group call, the MCPTT client shall comply with the procedures in subclause 6.2.8.1.9;

3) if the MCPTT user has requested the origination of a broadcast group call, the MCPTT client shall comply with the procedures in subclause 6.2.8.2;

4) shall include the g.3gpp.mcptt media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

5) 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];

6) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP INVITE request;

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

8) should include the "timer" option tag in the Supported header field;

9) 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";

10) shall set the Request-URI of the SIP INVITE request to the public service identity identifying the participating MCPTT function serving the MCPTT user;

NOTE 1: The MCPTT client is configured with public service identity identifying the participating MCPTT function serving the MCPTT user.

11) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [4];

12) if the MCPTT client emergency group state for this group is set to "MEG 2: in-progress" or "MEG 4: confirm-pending", the MCPTT client shall include the Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.2;

13) if the MCPTT client imminent peril group state for this group is set to "MIG 2: in-progress" or "MIG 4: confirm-pending" shall include the Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.12;

14) shall contain in an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with:

a) the <session-type> element set to a value of "prearranged";

b) the <mcptt-request-uri> element set to the group identity;

c) the <mcptt-client-id> element set to the MCPTT client ID of the originating MCPTT client; and

NOTE 2: The MCPTT client does not include the MCPTT ID of the originating MCPTT user in the body, as this will be inserted into the body of the SIP INVITE request that is sent from the originating participating MCPTT function.

d) if the group identity can be determined to be a TGI and if the MCPTT client can associate the TGI with a MCPTT group ID, the <associated-group-id> element set to the MCPTT group ID;

NOTE 3: The text "can associate the TGI with a MCPTT group ID" means that the MCPTT client is able to determine that there is a constituent group of the temporary group that it is a member of.

NOTE 4: The MCPTT client is informed about temporary groups and regouping of MCPTT groups that the user is a member of as specified in 3GPP TS 24.481 [31].

NOTE 5: If the MCPTT user selected a TGI where there are several MCPTT groups where the MCPTT user is a member, the MCPTT client selects one of those MCPTT groups.

15) shall include an SDP offer according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.1;

16) if an implicit floor request is required, shall indicate this as specified in subclause 6.4; and

17) shall send the SIP INVITE request towards the MCPTT server according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP INVITE request, the MCPTT client:

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

2) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested" or "MEGC 3: emergency-call-granted" or the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted", the MCPTT client shall perform the actions specified in subclause 6.2.8.1.4; and

3) may subscribe to the conference event package as specified in subclause 10.1.3.1.

On receiving a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request:

1) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested" or "MEGC 3: emergency-call-granted"; or

2) if the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted";

the MCPTT client shall perform the actions specified in subclause 6.2.8.1.5.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.1.13.

10.1.1.2.1.2 Client terminating procedures

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.

Upon receipt of an initial SIP INVITE request, the MCPTT client shall follow the procedures for termination of multimedia sessions in the IM CN subsystem as specified in 3GPP TS 24.229 [4] with the clarifications below.

The MCPTT client:

1) may reject the SIP INVITE request if either of the following conditions are met:

   a) MCPTT client does not have enough resources to handle the call; or

   b) any other reason outside the scope of this specification;

2) if the SIP INVITE request is rejected in step 1), shall respond toward participating MCPTT function either with appropriate reject code as specified in 3GPP TS 24.229 [4] and warning texts as specified in subclause 4.4.2 or with SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure and skip the rest of the steps of this subclause;

NOTE: If the SIP INVITE request contains an emergency indication or imminent peril indication, the MCPTT client can by means beyond the scope of this specification choose to accept the request.

3) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

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

   a) should display to the MCPTT user an indication that this is a SIP INVITE request for an MCPTT emergency group call and:

      i) should display the MCPTT ID of the originator of the MCPTT emergency group call contained in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body;

      ii) should display the MCPTT group identity of the group with the emergency condition contained in the <mcptt-calling-group-id> element; and

      iii) if the <alert-ind> element is set to "true", should display to the MCPTT user an indication of the MCPTT emergency alert and associated information;

   b) shall set the MCPTT emergency group state to "MEG 2: in-progress";

   c) shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; and

   d) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-gc-capable"; otherwise

5) if the SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "true":

   a) should display to the MCPTT user an indication that this is a SIP INVITE request for an MCPTT imminent peril group call and:

i) should display the MCPTT ID of the originator of the MCPTT imminent peril group call contained in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

ii) should display the MCPTT group identity of the group with the imminent peril condition contained in the <mcptt-calling-group-id> element; and

b) shall set the MCPTT imminent peril group state to "MIG 2: in-progress";

6) may display to the MCPTT user the MCPTT ID of the inviting MCPTT user;

7) shall perform the automatic commencement procedures specified in subclause 6.2.3.1.2 if one of the following conditions are met:

a) SIP INVITE request contains an Answer-Mode header field with the value "Auto" and the MCPTT service setting at the invited MCPTT client for answering the call is set to automatic commencement mode; or

b) SIP INVITE request contains an Answer-Mode header field with the value "Auto" and the MCPTT service setting at the invited MCPTT client for answering the call is set to manual commencement mode, yet the invited MCPTT client allows the call to be answered with automatic commencement mode;

8) shall perform the manual commencement procedures specified in subclause 6.2.3.2.2 if one of the following conditions are met:

a) SIP INVITE request contains an Answer-Mode header field with the value "Manual" and the MCPTT service setting at the invited MCPTT client for answering the call is to use manual commencement mode; or

b) SIP INVITE request contains an Answer-Mode header field with the value "Manual" and the MCPTT service setting at the invited MCPTT client for answering the call is set to automatic commencement mode, yet the invited MCPTT client allows the call to be answered with manual commencement mode; and

9) when the SIP 200 (OK) response to the SIP INVITE request is sent, may subscribe to the conference event package as specified in subclause 10.1.3.1.

10.1.1.2.1.3 MCPTT upgrade to in-progress emergency or imminent peril

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

Upon receiving a request from an MCPTT user to upgrade the MCPTT group session to an emergency condition or an imminent peril condition on an MCPTT prearranged group, the MCPTT client shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [4], with the clarifications given below.

1) if the MCPTT user is requesting to upgrade the MCPTT group session to an in-progress emergency group state and this is an unauthorised request for an MCPTT emergency call as determined by the procedures of subclause 6.2.8.1.8, the MCPTT client:

a) should indicate to the MCPTT user that they are not authorised to upgrade the MCPTT group session to an in-progress emergency group state; and

b) shall skip the remaining steps of the current subclause;

2) if the MCPTT user is requesting to upgrade the MCPTT group session to an in-progress imminent peril state and this is an unauthorised request for an MCPTT imminent peril group call as determined by the procedures of subclause 6.2.8.1.8, the MCPTT client:

a) should indicate to the MCPTT user that they are not authorised to upgrade the MCPTT group session to an in-progress imminent peril group state; and

b) shall skip the remaining steps of the current subclause;

3) if the MCPTT user has requested to upgrade the MCPTT group session to an MCPTT emergency call, the MCPTT client:

a) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.1; and

b) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.2.

4) if the MCPTT user has requested to upgrade the MCPTT group session to an MCPTT imminent peril call, the MCPTT client:

   a) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.9; and

   b) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.12;

5) if the SIP re-INVITE request is to be sent within an on-demand session, shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.2.1;

6) if the SIP re-INVITE request is to be sent within a pre-established session, shall include an SDP offer in the SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session;

NOTE: The SIP re-INVITE request can be sent within an on-demand session or a pre-established session. If the SIP re-INVITE request is sent within a pre-established session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

7) if an implicit floor request is required, shall indicate this as specified in subclause 6.4; and

8) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP re-INVITE request the MCPTT client:

1) shall interact with the user plane as specified in 3GPP TS 24.380 [5]; and

2) shall perform the actions specified in subclause 6.2.8.1.4.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.1.13.

On receiving a SIP 4xx response, SIP 5xx response or a SIP 6xx response to the SIP re-INVITE request the MCPTT client shall perform the actions specified in subclause 6.2.8.1.5.

10.1.1.2.1.4 MCPTT in-progress emergency cancel

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

Upon receiving a request from an MCPTT user to cancel the in-progress emergency condition on a prearranged MCPTT group, the MCPTT client shall generate a SIP re-INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) if the MCPTT user is not authorised to cancel the in-progress emergency group state of the MCPTT group as determined by the procedures of subclause 6.2.8.1.7, the MCPTT client:

   a) should indicate to the MCPTT user that they are not authorised to cancel the in-progress emergency group state of the MCPTT group; and

   b) shall skip the remaining steps of the current subclause;

2) shall, if the MCPTT user is cancelling an in-progress emergency condition and optionally an MCPTT emergency alert originated by the MCPTT user, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.3;

3) shall, if the MCPTT user is cancelling an in-progress emergency condition and an MCPTT emergency alert originated by another MCPTT user, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.14;

4) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with:

   a) the <session-type> element set to a value of "prearranged"; and

b) the <mcptt-request-uri> element set to the group identity;

NOTE 1: The MCPTT ID of the originating MCPTT user is not included in the body, as this will be inserted into the body of the SIP INVITE request that is sent by the originating participating MCPTT function.

5) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP re-INVITE request according to IETF RFC 3840 [16];

6) if the SIP re-INVITE request is to be sent within an on-demand session, shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.2.1;

7) if the SIP re-INVITE request is to be sent within a pre-established session, shall include an SDP offer in the SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session;

NOTE 2: The SIP re-INVITE request can be sent within an on-demand session or a pre-established session. If the SIP re-INVITE request is sent within a pre-established session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

8) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.2; and

9) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP re-INVITE request, the MCPTT client:

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

2) shall set the MCPTT emergency group state of the group to "MEG 1: no-emergency";

3) shall set the MCPTT emergency group call state of the group to "MEGC 1: emergency-gc-capable"; and

4) if the MCPTT emergency alert state is set to "MEA 4: Emergency-alert-cancel-pending", the sent SIP re-INVITE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body and the SIP 2xx response to the SIP request for a priority group call does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", shall set the MCPTT emergency alert state to "MEA 1: no-alert".

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.1.13.

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request:

1) shall set the MCPTT emergency group state as "MEG 2: in-progress";

2) if the SIP 4xx response, SIP 5xx response or SIP 6xx response contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to a value of "true" and the sent SIP re-INVITE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated"; and

3) if the SIP 4xx response, SIP 5xx response or SIP 6xx response did not contain an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element and did not contain an <originated-by> element, the MCPTT emergency alert (MEA) state shall revert to its value prior to entering the current procedure.

NOTE 3: If the in-progress emergency group state cancel request is rejected, the state of the session does not change, i.e. continues with MCPTT emergency group call level priority.

10.1.1.2.1.5 MCPTT in-progress imminent peril cancel

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

Upon receiving a request from an MCPTT user to cancel the in-progress imminent peril condition on a prearranged MCPTT group, the MCPTT client shall generate a SIP re-INVITE request by following the procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) if the MCPTT user is not authorised to cancel the in-progress imminent peril group state of the MCPTT group as determined by the procedures of subclause 6.2.8.1.10, the MCPTT client:

   a) should indicate to the MCPTT user that they are not authorised to cancel the in-progress imminent peril group state of the MCPTT group; and

   b) shall skip the remaining steps of the current subclause;

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.11; and

3) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.12;

4) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with:

   a) the <session-type> element set to a value of "prearranged"; and

   b) the <mcptt-request-uri> element set to the group identity;

NOTE 1: The MCPTT ID of the originating MCPTT user is not included in the body, as this will be inserted into the body of the SIP re-INVITE request that is sent by the originating participating MCPTT function.

5) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP re-INVITE request according to IETF RFC 3840 [16];

6) if the SIP re-INVITE request is to be sent within an on-demand session, shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.2.1;

7) if the SIP re-INVITE request is to be sent within a pre-established session, shall include an SDP offer in the SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session; and

NOTE 2: The SIP re-INVITE request can be sent within an on-demand session or a pre-established session. If the SIP re-INVITE request is sent within a pre-established session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

8) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP re-INVITE request, the MCPTT client:

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

2) shall set the MCPTT imminent peril group state of the group to "MIG 1: no-imminent-peril"; and

3) shall set the MCPTT imminent peril group call state of the group to "MIGC 1: imminent-peril-gc-capable".

On receiving a SIP 4xx, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request:

1) if the SIP 4xx response, SIP 5xx response or SIP 6xx response:

   a) contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <imminentperil-ind> element set to a value of "true"; or

   b) does not contain an application/vnd.3gpp.mcptt-info+xml MIME body with an <imminentperil-ind> element;

then the MCPTT client shall set the MCPTT imminent peril group state as "MIG 2: in-progress".

NOTE 3: This is the case where the MCPTT client requested the cancellation of the MCPTT imminent peril in-progress state and was rejected.

10.1.1.2.1.6 MCPTT client receives SIP re-INVITE request

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

Upon receipt of a SIP re-INVITE request the MCPTT client:

1) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "true":

   a) should display to the MCPTT user the MCPTT ID of the originator of the MCPTT emergency group call and an indication that this is an MCPTT emergency group call;

   b) if the <mcpttinfo> element containing the <mcptt-Params> element contains an <alert-ind> element set to "true", should display to the MCPTT user an indication of the MCPTT emergency alert and associated information;

   c) shall set the MCPTT emergency group state to "MEG 2: in-progress";

   d) shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; and

   e) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-gc-capable";

2) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "true":

   a) should display to the MCPTT user the MCPTT ID of the originator of the MCPTT imminent peril group call and an indication that this is an MCPTT imminent peril group call; and

   b) shall set the MCPTT imminent peril group state to "MIG 2: in-progress";

3) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "false":

   a) should display to the MCPTT user the MCPTT ID of the MCPTT user cancelling the MCPTT emergency group call;

   b) if the <mcpttinfo> element containing the <mcptt-Params> element contains an <alert-ind> element set to "false":

      i) should display to the MCPTT user an indication of the MCPTT emergency alert cancellation and the MCPTT ID of the MCPTT user cancelling the MCPTT emergency alert; and

      ii) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body including an <originated-by> element:

         A) should display to the MCPTT user the MCPTT ID contained in the <originated-by> element of the MCPTT user that originated the MCPTT emergency alert; and

         B) if the MCPTT ID contained in the <originated-by> element is the MCPTT ID of the receiving MCPTT user shall set the MCPTT emergency alert state to "MEA 1: no-alert";

   c) shall set the MCPTT emergency group state to "MEG 1: no-emergency"; and

   d) if the MCPTT emergency group call state of the group is set to "MEGC 3: emergency-call-granted", shall set the MCPTT emergency group call state of the group to "MEGC 1: emergency-gc-capable";

4) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "false":

   a) should display to the MCPTT user the MCPTT ID of the MCPTT user cancelling the MCPTT imminent peril group call and an indication that this is an MCPTT imminent peril group call;

   b) shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; and

   c) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-gc-capable";

5) shall check if a Resource-Priority header field is included in the incoming SIP re-INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

6) shall accept the SIP re-INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [4];

7) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP 200 (OK) response;

8) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP 200 (OK) response;

9) if the SIP re-INVITE request was received within an on-demand session, shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP re-INVITE request according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.2;

10) if the SIP re-INVITE request was received within a pre-established session, shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session;

NOTE: The SIP re-INVITE request can be received within an on-demand session or a pre-established session. If the SIP re-INVITE request is received within a pre-established session, the media-level section for the MCPTT speech media stream and the media-level section of the media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

11) shall send the SIP 200 (OK) response towards the MCPTT server according to rules and procedures of 3GPP TS 24.229 [4]; and

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

10.1.1.2.2 Prearranged group call using pre-established session

10.1.1.2.2.1 Client originating procedures

Upon receiving a request from an MCPTT user to establish an MCPTT group session using an MCPTT group identity identifying a prearranged MCPTT group within the pre-established session, the MCPTT client shall generate a SIP REFER request as specified in IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27], and in accordance with the UE procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client shall follow the procedures specified in subclause 10.1.2.2.2.1 with the clarification in step 3) of subclause 10.1.2.2.2.1 that:

1) the <entry> element in the application/resource-lists MIME body shall contain a "uri" attribute set to the prearranged MCPTT group identity;

2) the <session-type> element of the application/vnd.3gpp.mcptt-info MIME body in the hname "body" URI header field shall be set to a value of "prearranged"; and

3) if the MCPTT user has requested the origination of a broadcast group call, the MCPTT client shall comply with the procedures in subclause 6.2.8.2.

10.1.1.2.2.2 Client terminating procedures

Upon receiving a SIP re-INVITE request within a pre-established Session without an associated MCPTT session or when generating SIP responses to the SIP re-INVITE request, the MCPTT client shall follow the procedures in subclause 10.1.1.2.1.2.

NOTE: In subclause 10.1.1.2.1.2, the reader is assumed to replace occurrences of SIP INVITE request with SIP re-INVITE request.

10.1.1.2.3 End group call

10.1.1.2.3.1 Client originating procedures on-demand

When an MCPTT client wants to leave the MCPTT session that has been established using on-demand session, the MCPTT client shall follow the procedures as specified in subclause 6.2.4.1.

10.1.1.2.3.2 Client originating procedures using pre-established session

When an MCPTT client wants to leave the MCPTT session within a pre-established session, the MCPTT client shall follow the procedures as specified in subclause 6.2.4.2.

10.1.1.2.3.3 Client terminating procedures

Upon receiving a SIP BYE request for releasing the prearranged MCPTT group call, the MCPTT client shall follow the procedures as specified in subclause 6.2.6.

10.1.1.2.4 Re-join procedure

10.1.1.2.4.1 On demand session establishment

Upon receiving a request from an MCPTT user to re-join an ongoing MCPTT session or triggered by coming back from out of coverage, the MCPTT client shall generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

NOTE: How an MCPTT client is informed whether it comes back from out of coverage is out of scope of present document.

The MCPTT client shall follow the procedures specified in subclause 10.1.1.2.1.1 with the clarification in step 10) of subclause 10.1.1.2.1.1 that the Request-URI of the SIP INVITE request shall contain a URI of the MCPTT session identity to re-join.

10.1.1.2.4.2 Pre-established session

Upon receiving a request from an MCPTT user to re-join an ongoing MCPTT session within the pre-established session or triggered by coming back from out of coverage, the MCPTT client shall generate a SIP REFER request as specified in IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27], and in accordance with the UE procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client shall follow the procedures specified in subclause 10.1.1.2.2.1 with the clarification in step 3) of subclause 10.1.2.2.2.1 that the Refer-To header field of the SIP REFER request:

1) shall contain a URI of the MCPTT session identity to re-join; and

2) shall contain a Content-Type URI header field containing an application/vnd.3gpp.mcptt-info+xml MIME type of the "body" URI header field and the body URI header field containing the <mcptt-info> element with the <mcptt-Params> element and with the <session-type> element set to a value of "prearranged".

10.1.1.3 Participating MCPTT function procedures

10.1.1.3.1 Originating procedures

10.1.1.3.1.1 On demand prearranged group call

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 24.484 [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 23.379 [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 with the clarification that if an <MKFC-GKTPs> element was contained in the received SIP 200 (OK) response it is not included in the generated SIP 200 (OK) response;

NOTE 9: If an <MKFC-GKTPs> element is received, the participating MCPTT function essentially ignores it and does not forward it, resulting in unicast media plane transmission being used for the originating client.

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;

10.1.1.3.1.2 Prearranged group call using pre-established session

Upon receipt of a "SIP REFER request for a pre-established session", with:

1) the Refer-To header field containing a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [20] containing an <entry> element with a "uri" attribute containing a SIP-URI set to a pre-arranged group identity;

2) a body" URI header field of the SIP-URI specified above containing an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element set to "prearranged"; and

3) a Content-ID header field set to the "cid" URL;

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 1: If the application/vnd.3gpp.mcptt-info MIME body included in the SIP REFER request as described at the top of the present subclause contains an <emergency-ind> element or <imminentperil-ind> element 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 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 24.484 [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 and shall not continue with the rest of the steps;

3) shall determine the MCPTT ID of the calling user from public user identity in the P-Asserted-Identity header field of the SIP REFER request;

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.

4) if the participating MCPTT function cannot find a binding between the public user identity and an MCPTT ID or if the validity period of an existing binding has expired, then the participating MCPTT function shall reject the SIP REFER request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

5) 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 REFER request for pre-established session" 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;

6) if the "SIP REFER request for a pre-established session" contained a Refer-Sub header field containing "false" value and a Supported header field containing "norefersub" value, shall handle the SIP REFER request as specified in 3GPP TS 24.229 [4], IETF RFC 3515 [25] as updated by IETF RFC 6665 [26], and IETF RFC 4488 [22] without establishing an implicit subscription;

7) if received SIP REFER request includes an application/vnd.3gpp.mcptt-info+xml MIME body with an <emergency-ind> element included or an <imminentperil-ind> element included, shall validate the request as described in subclause 6.3.2.1.8.3;

8) if the SIP REFER request contains in the application/vnd.3gpp.mcptt-info+xml MIME body:

   a) an <emergency-ind> element set to a value of "true" and this is an unauthorised request for an MCPTT emergency group call as determined by subclause 6.3.2.1.8.1;

   b) an <alert-ind> element set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as determined by subclause 6.3.2.1.8.2; or

   c) an <imminentperil-ind> element set to a value of "true" and this is an unauthorised request for an MCPTT imminent peril group call as determined by subclause 6.3.2.1.8.1;

   then shall reject the SIP REFER request with a SIP 403 (Forbidden) response and skip the rest of the steps;

9) shall retrieve the group identity within the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL contained in the Refer-To header field of the SIP REFER request;

10) shall determine the public service identity of the controlling MCPTT function associated with the group identity in the application/resource-lists MIME body referenced by the Refer-To header of the SIP REFER request. If the participating MCPTT function is unable to identify the controlling MCPTT function associated with the group identity, it shall reject the REFER request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

NOTE 3: The public service identity can identify the controlling function in the primary MCPTT system or a partner MCPTT system.

NOTE 4: 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 document.

11) if the user identified by the MCPTT ID is not affiliated to the group identified in the SIP REFER request 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;

12) if the actions for implicit affiliation specified in step 11) 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 REFER request 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 5: N2 is the total number of MCPTT groups that an MCPTT user can be affiliated to simultaneously as specified in 3GPP TS 23.379 [3].

NOTE 6: 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.

13) shall generate a final SIP 200 (OK) response to the "SIP REFER request for a pre-established session" according to 3GPP TS 24.229 [4];

NOTE 7: In accordance with IETF RFC 4488 [22], the participating MCPTT function inserts the Refer-Sub header field containing the value "false" in the SIP 200 (OK) response to the SIP REFER request to indicate that it has not created an implicit subscription.

14) shall send the response to the "SIP REFER request for a pre-established session" towards the MCPTT client according to 3GPP TS 24.229 [4];

15) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.4;

16) shall set the Request-URI of the SIP INVITE request to the public service identity of the controlling MCPTT function associated with the group identity;

17) shall copy the group identity from the "uri" attribute of the <entry> element of the application/resource-lists MIME body pointed to by the "cid" URL in the Refer-to header field of the SIP REFER request, to the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body in the SIP INVITE request;

18) if the received SIP REFER request contained a Resource-Priority header field, shall include in the outgoing SIP INVITE request 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 received SIP REFER 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.

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

Upon receiving SIP provisional responses for the SIP INVITE request the participating MCPTT function:

1) shall discard the received SIP responses without forwarding them.

Upon receipt of a SIP 302 (Moved Temporarily) response to the 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 in the SIP INVITE request an SDP offer based upon the SDP offer negotiated during the pre-established session establishment, any subsequent pre-established session modification and the SDP offer (if any) included in the"body" URI parameter of the SIP-URI contained in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field in the incoming SIP REFER request from the MCPTT client; and

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

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

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

2) 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; and

3) if the received SIP 2xx response was in response to a request for an MCPTT group call containing a Resource-Priority header field populated for an MCPTT emergency group call or MCPTT imminent peril group call as specified in subclause 6.3.2.1.8.4 and does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149":

   a) shall generate a SIP re-INVITE request to be sent towards the MCPTT client within the pre-established session as specified in subclause 6.3.2.1.8.5; and

b) shall send the SIP re-INVITE request towards the MCPTT client according to 3GPP TS 24.229 [4].

NOTE 8: There are two cases covered in the handling of the received SIP 2xx response above. The first case is when the SIP INVITE request sent to the controlling MCPTT function contained a Resource-Priority header field populated appropriately to request emergency level or imminent peril level priority but did not contain in the application/vnd.3gpp.mcptt-info+xml MIME body either an <emergency-ind> element or an <imminentperil-ind> element. The second case is when the SIP INVITE request sent to the controlling MCPTT function contained a Resource-Priority header field and contained either an <emergency-ind> element or an <imminentperil-ind> element. In either case, the received SIP 2xx response did not warn of a pending SIP INFO request.

Upon receiving a SIP INFO request from the controlling MCPTT function within the dialog of the SIP INVITE request for an MCPTT emergency call or MCPTT imminent peril call, the participating MCPTT function:

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

2) shall generate a SIP re-INVITE request to be sent towards the MCPTT client within the pre-established session as specified in subclause 6.3.2.1.8.5; and

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

NOTE 9: This is the case where the SIP REFER request previously received from the MCPTT client contained a Resource-Priority header field populated for an MCPTT emergency group call or MCPTT imminent peril group call as specified in subclause 6.3.2.1.8.4 but was also a request either an MCPTT emergency group call or an MCPTT imminent peril group call.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request in step 19) the participating MCPTT function:

1) 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; and

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

10.1.1.3.1.3 Reception of a SIP re-INVITE request from served MCPTT client

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

Upon receipt of a SIP re-INVITE request for an MCPTT session identifying an on-demand prearranged MCPTT group session, 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 re-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 skip the rest of the steps;

NOTE 1: If the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "true", the participating MCPTT function can choose to accept the request.

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. Otherwise, continue with the rest of the steps;

NOTE 2: If the received SIP re-INVITE request is received within a pre-established session associated with an MCPTT group session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

3) shall generate an outgoing SIP re-INVITE request as specified in subclause 6.3.2.1.9;

4) shall, if the SIP re-INVITE request was received within an on-demand session, include in the SIP re-INVITE request an SDP offer based on the SDP offer in the received SIP re-INVITE request as specified in subclause 6.3.2.1.1;

5) shall, if the SIP re-INVITE request was received within a pre-established session, include in the SIP re-INVITE request an SDP offer based upon the previously negotiated SDP for the pre-established session as specified in subclause 6.3.2.1.1.2;

6) if the received SIP re-INVITE request contains a Resource-Priority header field, shall include a Resource-Priority header field with the contents set as in the received Resource-Priority header field; and

NOTE 3: The controlling MCPTT function will determine the validity of the Resource-Priority header field.

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

Upon receipt of a SIP 2xx response to the above SIP re-INVITE request in step 7) the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as specified in the subclause 6.3.2.1.5.2;

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

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

4) shall copy the contents 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;

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

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

Upon receipt of a SIP 403 (Forbidden) response to the above SIP INVITE request in step 7) the participating MCPTT function:

1) shall generate a SIP 403 (Forbidden) response according to 3GPP TS 24.229 [4];

2) shall copy, if included in the received SIP 403 (Forbidden) response, the application/vnd.3gpp.mcptt-info+xml MIME body MIME body to the outgoing SIP (Forbidden) response;

3) shall include Warning header field(s) that were received in the incoming SIP 403 (Forbidden) response;

4) shall forward the SIP 403 (Forbidden) response to the MCPTT client according to 3GPP TS 24.229 [4]; and

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

10.1.1.3.2 Terminating Procedures

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 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 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;

NOTE 2: If an <MKFC-GKTPs> element is received, the participating MCPTT function essentially ignores it and does not forward it, resulting in unicast media plane transmission being used for the terminating client.

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".

10.1.1.3.3 End group call at the originating participating MCPTT function

10.1.1.3.3.1 Receipt of SIP BYE request for ending group call on-demand

Upon receiving from the MCPTT client a SIP BYE request the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.1.6.

10.1.1.3.3.2 Receipt of SIP REFER "BYE" request for ending group call using pre-established session

Upon receiving from the MCPTT client a SIP REFER request when using a pre-established session with the method SIP-URI parameter set to value "BYE" in the URI in the Refer-To header field the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.1.7.

10.1.1.3.4 End group call at the terminating participating MCPTT function

10.1.1.3.4.1 Receipt of SIP BYE request for private call on-demand

Upon receiving a SIP BYE request from the controlling MCPTT function, the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.2.8.1.

10.1.1.3.4.2 Receipt of SIP BYE request when ongoing pre-established session

Upon receiving a SIP BYE request from the controlling MCPTT function and if the MCPTT session id refers to an MCPTT user that has a pre-established session with the participating MCPTT function, the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.2.8.2.

10.1.1.3.5 Re-join procedures

10.1.1.3.5.1 Originating procedures - on demand prearranged group call

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 shall follow the procedures specified in subclause 10.1.1.3.1.1 with the clarification in step 10) of subclause 10.1.1.3.1.1 that the Request-URI of the SIP INVITE request shall contain a URI of the MCPTT session identity which mapped to the MCPTT session identity provided in Request-URI header field of the "SIP INVITE request for originating participating MCPTT function".

10.1.1.3.5.2 Originating procedures - prearranged group call using pre-established session

Upon receipt of a "SIP REFER request for a pre-established session", with the Refer-To header containing an application/vnd.3gpp.mcptt-info+xml MIME type content in a "body" URI header field and with the <session-type> element set to "prearranged" the participating MCPTT function shall follow the procedures specified in subclause 10.1.1.3.1.2 with the clarification in step 16) of subclause 10.1.1.3.1.2 that the Request-URI of the SIP INVITE request shall contain a URI of the MCPTT session identity which mapped to the MCPTT session identity provided in the Refer-to header field of the "SIP REFER request for a pre-established session".

10.1.1.3.6 Reception of a SIP re-INVITE request for terminating MCPTT client for priority call

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.

Upon receipt of a SIP re-INVITE request for a terminating MCPTT client of a MCPTT group containing an emergency indication or imminent peril indication, the participating MCPTT function:

1) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

2) shall generate an outgoing SIP re-INVITE request as specified in subclause 6.3.2.2.10;

3) shall include in the SIP re-INVITE request an SDP offer based on the SDP offer in the received SIP re-INVITE request as specified in subclause 6.3.2.2.1; and

4) shall send the SIP re-INVITE request towards the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the above SIP re-INVITE request sent to the MCPTT client, the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as described in the subclause 6.3.2.2.4.2;

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 6.3.2.2.2.1;

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

4) shall forward the SIP 200 (OK) response according to 3GPP TS 24.229 [4].

10.1.1.4 Controlling MCPTT function procedures

10.1.1.4.1 Originating Procedures

10.1.1.4.1.1 INVITE targeted to an MCPTT client

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) void

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.

10.1.1.4.1.2 INVITE targeted to the non-controlling MCPTT function of an MCPTT group

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) void

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 23.379 [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 24.481 [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.

10.1.1.4.2 Terminating Procedures

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:

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 controlling 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 skip 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 an MCPTT emergency group call as determined by subclause 6.3.3.1.13.2, or for originating an MCPTT imminent peril group call as determined by subclause 6.3.3.1.13.5, the controlling MCPTT function can according to local policy choose to accept the request.

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;

3) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

4) if received SIP INVITE request includes an application/vnd.3gpp.mcptt-info+xml MIME body with an <emergency-ind> element included or an <imminentperil-ind> element included, shall validate the request as described in subclause 6.3.3.1.17;

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;

6) if the result of the initial processing in subclause 6.3.5.2 was:

   a) that authorization of the MCPTT ID is required at a non-controlling MCPTT function of an MCPTT group is required, perform the actions in subclause 6.3.3.1.13.7 and do not continue with the rest of the steps in this subclause; and

   b) that a SIP 3xx, 4xx, 5xx or 6xx response to the "SIP INVITE request for controlling MCPTT function of an MCPTT group" has been sent, do not continue with the rest of the steps in this subclause;

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;

10) if the SIP INVITE request contains an unauthorised request for an MCPTT emergency group call as determined by subclause 6.3.3.1.13.2:

   a) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response as specified in subclause 6.3.3.1.14; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

11) if the SIP INVITE request contains an unauthorised request for an MCPTT imminent peril group call as determined by subclause 6.3.3.1.13.5, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response with the following clarifications:

   a) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "false"; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

12) if a Resource-Priority header field is included in the SIP INVITE request:

a) if the Resource-Priority header field is set to the value indicated for emergency calls and the SIP INVITE request does not contain an emergency indication and the in-progress emergency state of the group is set to a value of "false", shall reject the SIP INVITE request with a SIP 403 (Forbidden) response and skip the rest of the steps; or

b) if the Resource-Priority header field is set to the value indicated for imminent peril calls and the SIP INVITE request does not contain an imminent peril indication and the in-progress imminent peril state of the group is set to a value of "false", shall reject the SIP INVITE request with a SIP 403 (Forbidden) response and skip the rest of the steps;

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;

b) if the user identified by the MCPTT ID is not authorised to initiate the prearranged group session as specified in subclause 6.3.5.4, shall send a SIP 403 (Forbidden) response with the warning text set to: "119 user is not authorised to initiate the group call" in a Warning header field as specified in subclause 4.4 and skip the rest of the steps below;

c) if the received SIP INVITE request contains 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 subclause 6.3.3.1.13.5 and the MCPTT user is eligible to be implicitly affiliated with the MCPTT group as determined as determined in step 13) a) iv) above, shall perform the implicit affiliation as specified in subclause 9.2.2.3.7;

d) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

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;

f) if the group identity in the "SIP INVITE request for controlling MCPTT function of an MCPTT group" is a TGI:

i) shall for each of the constituent MCPTT groups homed on the primary MCPTT system:

A) if the controlling MCPTT function does not own the MCPTT group identified by the MCPTT group ID, then generate a SIP INVITE request towards the MCPTT server that owns the MCPTT group identity by following the procedures in subclause 10.1.1.4.1.2; and

NOTE 2: The MCPTT server that the SIP INVITE request is sent to acts as a non-controlling MCPTT function;

B) if the controlling MCPTT function owns the MCPTT group identified by the MCPTT group ID then:

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

II) invite each group member determined in step A) above, to the group session, as specified in subclause 10.1.1.4.1.1; and

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

ii) shall for each of the constituent MCPTT groups homed on the partner MCPTT system generate a SIP INVITE request for the MCPTT group identity homed on the partner MCPTT system as specified in subclause 10.1.1.4.1.2; and

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;

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

A) shall cache the information that the MCPTT user has initiated an MCPTT emergency call;

B) if the received SIP INVITE contains an alert indication set to a value of "true" and this is an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, shall cache the information that the MCPTT user has initiated an MCPTT emergency alert; and

C) if the in-progress emergency state of the group is set to a value of "false":

I) shall set the value of the in-progress emergency state of the group to "true"; and

II) shall start timer TNG2 (in-progress emergency group call timer) and handle its expiry as specified in subclause 6.3.3.1.16;

iv) if the in-progress emergency state of the group is set to a value of "false" and if the received SIP INVITE request contains an imminent peril indication set to a value of "true", the controlling MCPTT function shall:

A) shall cache the information that the MCPTT user has initiated an MCPTT imminent peril call; and

B) if the in-progress imminent peril state of the group is set to a value of "false", shall set the in-progress imminent peril state of the group to a value of "true";

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

14) if the MCPTT group call is ongoing then:

a) if:

i) the user identified by the MCPTT ID in the SIP INVITE request 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 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;

b) if the user identified by the MCPTT ID in the SIP INVITE request is not authorised to join the prearranged group session as specified in subclause 6.3.5.3, shall send a SIP 403 (Forbidden) response with the warning text set to "121 user is not allowed to join the group call" in a Warning header field as specified in subclause 4.4 and skip the rest of the steps below;

c) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

d) if <on-network-max-participant-count> as specified in 3GPP TS 24.481 [31] is already reached:

i) if, according to local policy, the user identified by the MCPTT ID in the SIP INVITE request is deemed to have a higher priority than an existing user in the group session, may remove a participant from the session by following subclause 10.1.1.4.4.3, and skip the next step; and

NOTE 3: The local policy for deciding whether to admit a user to a call that has reached its maximum amount of participants can include the <user-priority> and the <participant-type> of the user as well as other information of the user from the group document as specified in 3GPP TS 24.481 [31]. The local policy decisions can also include taking into account whether the imminent-peril indicator or emergency indicator was received in the SIP INVITE request.

ii) shall return a SIP 486 (Busy Here) response with the warning text set to "122 too many participants" to the originating network as specified in subclause 4.4 and skip the rest of the steps;

e) if the received SIP INVITE request contains 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 subclause 6.3.3.1.13.5 and the MCPTT user is eligible to be implicitly affiliated with the MCPTT group as determined in step 14) a) iv) above, shall perform the implicit affiliation as specified in subclause 9.2.2.3.7;

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

i) shall cache the information that the MCPTT user has initiated an MCPTT emergency call;

ii) if the received SIP INVITE contains an alert indication set to a value of "true" and this is an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, shall cache the information that the MCPTT user has initiated an MCPTT emergency alert;

iii) if the in-progress emergency state of the group is set to a value of "false":

A) shall set the value of the in-progress emergency state of the group to "true";

B) shall start timer TNG2 (in-progress emergency group call timer) and handle its expiry as specified in subclause 6.3.3.1.16; and

C) shall generate SIP re-INVITE requests for the MCPTT emergency group call to the other call participants of the MCPTT group as specified in subclause 6.3.3.1.6;

iv) if the in-progress imminent peril state of the group is set to a value of "true":

A) for each of the other affiliated member of the group generate a SIP MESSAGE request notification of the MCPTT user's imminent peril indication as specified in subclause 6.3.3.1.11, setting the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "true"; and

B) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4]; and

v) upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5];

g) if the in-progress emergency state of the group is set to a value of "false" and if the SIP INVITE request contains an imminent peril indication set to a value of "true", the controlling MCPTT function:

i) shall cache the information that the MCPTT user has initiated an MCPTT imminent peril call; and

ii) if the in-progress imminent peril state of the group is set to a value of "false":

A) shall set the in-progress imminent peril state of the group to a value of "true";

B) shall generate SIP re-INVITE requests for the MCPTT imminent peril group call to the other call participants of the MCPTT group as specified in subclause 6.3.3.1.15; and

C) upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

iii) if the in-progress imminent peril state of the group is set to a value of "true":

A) for each of the other affiliated member of the group generate a SIP MESSAGE request notification of the MCPTT user's imminent peril indication as specified in subclause 6.3.3.1.11, setting the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "true"; and

B) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4];

h) shall generate a SIP 200 (OK) response as specified in the subclause 6.3.3.2.4.2;

i) 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;

j) shall include in the SIP 200 (OK) response with the warning text set to "123 MCPTT session already exists" as specified in subclause 4.4;

k) if the received SIP re-INVITE request contains an alert indication set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

l) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "true" and if the in-progress emergency state of the group is set to a value of "true", shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

NOTE 4: In this case, the request was for an imminent peril call but a higher priority MCPTT emergency call was already in progress on the group. Hence, the imminent peril call request aspect of the request is denied but the request is granted with emergency level priority.

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

NOTE 5: Resulting media plane processing is completed before the next step is performed.

n) shall send the SIP 200 (OK) response towards the inviting MCPTT client or inviting non-controlling MCPTT function according to 3GPP TS 24.229 [4];

o) shall generate a notification to the MCPTT clients, which have subscribed to the conference state event package that the inviting MCPTT User has joined in the MCPTT group session, as specified in subclause 6.3.3.4;

NOTE 6: As a group document can potentially have a large content, the controlling MCPTT function can notify using content-indirection as defined in IETF RFC 4483 [32].

p) shall send a SIP NOTIFY request to each MCPTT client according to 3GPP TS 24.229 [4];

q) Upon receiving a SIP ACK to the above SIP 200 (OK) response and the SIP 200 (OK) response contained a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", shall follow the procedures in subclause 6.3.3.1.18; and

r) shall not continue with the rest of the subclause.

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;

2) shall include the warning text set to "122 too many participants" as specified in subclause 4,4 in the SIP 200 (OK) response, if the prearranged MCPTT group has more than <on-network-max-participant-count> members as specified in 3GPP TS 24.481 [31];

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";

5) if the SIP INVITE request contains an alert indication set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

6) if the received SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "true" and if the in-progress emergency state of the group is set to a value of "true", shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

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];

9) shall generate a notification to the MCPTT clients, which have subscribed to the conference state event package that the inviting MCPTT User has joined in the MCPTT group session, as specified in subclause 6.3.3.4; and

NOTE 8: As a group document can potentially have a large content, the controlling MCPTT function can notify using content-indirection as defined in IETF RFC 4483 [32].

10) shall send a SIP NOTIFY request to each MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 183 (Session Progress) response for a SIP INVITE request as specified in subclause 10.1.1.4.1.2 containing an indication of required group members, the timer TNG1 (acknowledged call setup timer) is running and all SIP 200 (OK) responses have been received to all SIP INVITE requests sent to MCPTT clients specified in subclause 10.1.1.4.1.1, then the controlling MCPTT function shall wait until the SIP 200 (OK) response has been received to the SIP INVITE request specified in subclause 10.1.1.4.1.2 before generating a SIP 200 (OK) response to the "SIP INVITE request for controlling MCPTT function of an MCPTT group".

Upon receiving a SIP 200 (OK) response for a SIP INVITE request as specified in subclause 10.1.1.4.1 that was sent to an affiliated and <on-network-required> group member as specified in 3GPP TS 24.481 [31]; and

1) if the MCPTT ID in the SIP 200 (OK) response matches to the MCPTT ID in the corresponding SIP INVITE request;

2) there are no outstanding SIP 200 (OK) responses to SIP INVITE requests which were sent to affiliated and <on-network-required> group members as specified in 3GPP TS 24.481 [31]; and

3) there is no outstanding SIP 200 (OK) response to a SIP INVITE request sent in subclause 10.1.1.4.1.2 where the SIP 183 (Session Progress) response contained an indication of required group members;

the controlling MCPTT function:

1) shall stop timer TNG1 (acknowledged call setup timer) as described in subclause 6.3.3.3;

2) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.3.2.3.2 before continuing with the rest of the steps;

3) shall include the warning text set to "122 too many participants" as specified in subclause 4.4 in the SIP 200 (OK) response, if all members were not invited because the prearranged MCPTT group has been exceeded the <on-network-max-participant-count> members as specified in 3GPP TS 24.481 [31];

4) 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;

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

NOTE 9: Resulting media plane processing is completed before the next step is performed.

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

7) shall generate a notification to the MCPTT clients, which have subscribed to the conference state event package that the inviting MCPTT user has joined in the MCPTT group session, as specified in subclause 6.3.3.4; and

NOTE 10: As a group document can potentially have a large content, the controlling MCPTT function can notify using content-indirection as defined in IETF RFC 4483 [32].

8) shall send the SIP NOTIFY request to the MCPTT clients 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;

2) shall include the warning text set to "122 too many participants" as specified in subclause 4.4 in the SIP 200 (OK) response, if all members were not invited because the prearranged MCPTT group has exceeded the <max-participant-count> members as specified in 3GPP TS 24.481 [31];

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) if the SIP INVITE request contains an alert indication set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

5) if the received SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "true" and if the in-progress emergency state of the group is set to a value of "true", shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

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];

8) shall generate a notification to the MCPTT clients, which have subscribed to the conference state event package that the inviting MCPTT user has joined in the MCPTT group session, as specified in subclause 6.3.3.4; and

NOTE 12: As a group document can potentially have a large content, the controlling MCPTT function can notify using content-indirection as defined in IETF RFC 4483 [32].

9) shall send the SIP NOTIFY request to the MCPTT clients according to 3GPP TS 24.229 [4].

Upon expiry of timer TNG1 (acknowledged call setup timer), if there are outstanding SIP 200 (OK) responses to SIP INVITE requests sent to affiliated and <on-network-required> group members as specified in 3GPP TS 24.481 [31], the controlling MCPTT function shall follow the procedures specified in subclause 6.3.3.3.

If timer TNG1 (acknowledged call setup timer) is running and a final SIP 4xx, 5xx or 6xx response is received from an affiliated and <on-network-required> group member as specified in 3GPP TS 24.481 [31], the controlling MCPTT function shall follow the relevant procedures specified in subclause 6.3.3.3.

If:

1) timer TNG1 (acknowledged call setup timer) is not running;

2) 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; and

3) a final SIP 4xx, 5xx or 6xx response is received from an invited MCPTT client;

then the controlling MCPTT function shall perform one of the following based on policy:

1) send the SIP final response towards the inviting MCPTT client, according to 3GPP TS 24.229 [4], if a SIP final response was received from all the other invited MCPTT clients and the SIP 200 (OK) response is not yet sent; or

2) remove the invited MCPTT client from the MCPTT Session as specified in subclause 6.3.3.1.5, if a SIP final response other than 2xx or 3xx was received from all the invited MCPTT clients and the SIP 200 (OK) response is already sent. The controlling MCPTT function may invite an additional member of the prearranged MCPTT group as specified in subclause 10.1.1.4.1 that has not already been invited, if the prearranged MCPTT group has more than <on-network-max-participant-count> members as specified in 3GPP TS 24.481 [31], and all members have not yet been invited.

If the group identity in the "SIP INVITE request for controlling MCPTT function of an MCPTT group" is a TGI and constituent MCPTT groups were invited as specified in subclause 10.1.1.4.1.2 and,

1) if all non-controlling MCPTT functions hosting the constituent MCPTT groups have responded with a SIP 2xx, SIP 3xx, SIP 4xx, SIP 5xx or SIP 6xx responses to the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group"; and

2) if all expected SIP INFO requests containing a floor request are received;

then the controlling MCPTT function shall indicate to the media plane that all final responses are received.

NOTE 13: If the SIP 200 (OK) response to the SIP INVITE request for non-controlling MCPTT function of an MCPTT group included the application/vnd.3gpp.mcptt-info+xml MIME body with the <floor-state> element set to "floor-taken", the controlling MCPTT function expects that the non-controlling MCPTT functions sends a SIP INFO request containing a floor request.

Upon receiving a SIP ACK to the SIP 200 (OK) response sent towards the inviting MCPTT client, and the SIP 200 (OK) response was sent with the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.18.

10.1.1.4.3 End group call at the terminating controlling MCPTT function

Upon receiving a SIP BYE request the controlling MCPTT function shall follow the procedures as specified in subclause 6.3.3.2.4.

10.1.1.4.4 End group call initiated by the controlling MCPTT function

10.1.1.4.4.1 General

This subclause describes the procedures of each functional entity for ending the group call initiated by the controlling MCPTT function.

10.1.1.4.4.2 SIP BYE request for releasing MCPTT session for a group call

When the MCPTT session for group call needs to be released as specified in subclause 6.3.8.1, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.5.

10.1.1.4.4.3 SIP BYE request toward a MCPTT client

When an MCPTT client needs to be removed from the MCPTT session (e.g. due to de-affiliation or admitting a higher priority user), the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.5.

After successful removing the MCPTT client from the MCPTT session, the controlling MCPTT function may generate a notification to the MCPTT clients, which have subscribed to the conference state event package that an MCPTT user has been removed from the MCPTT session, as specified in subclause 6.3.3.4 and send the SIP NOTIFY request to the MCPTT client according to 3GPP TS 24.229 [4].

10.1.1.4.5 Re-join procedures

10.1.1.4.5.1 Terminating procedures

Upon receipt of a SIP INVITE request that includes an MCPTT session identity of an ongoing MCPTT session in the Request-URI the controlling 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 controlling 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 an MCPTT emergency group call as determined by subclause 6.3.3.1.13.2, or for originating an MCPTT imminent peril group call as determined by subclause 6.3.3.1.13.5, the controlling MCPTT function can according to local policy choose to accept the request.

2) shall reject the SIP request with a SIP 404 (Not Found) response if the MCPTT group call represented by the MCPTT session identity in Request-URI header is not present;

3) 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. Otherwise, continue with the rest of the steps;

4) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

5) shall determine the MCPTT ID of the calling user;

6) if the user identified by the MCPTT ID is not authorised to join the prearranged group session as specified in subclause 6.3.5.3, shall send a SIP 403 (Forbidden) response with the warning text set to "121 user is not authorised to join the group call" in a Warning header field as specified in subclause 4.4. Otherwise continue with the rest of the steps below;

7) shall perform the actions on receipt of an initial SIP INVITE request as described in subclause 6.3.3.2.2;

8) if the user identified by the MCPTT ID is not affiliated to the MCPTT group ID associated with the MCPTT session identity as specified in subclause 6.3.3.5, 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;

9) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

10) if <on-network-max-participant-count> as specified in 3GPP TS 24.481 [31] is already reached:

   a) if, according to local policy, the user identified by the MCPTT ID in the SIP INVITE request is deemed to have a higher priority than an existing user in the group session, may remove a participant from the session by following subclause 10.1.1.4.4.3, and skip the next step; and

NOTE 2: The local policy for deciding whether to admit a user to a call that has reached its maximum amount of participants can include the <user-priority> and the <participant-type> of the user as well as other information of the user from the group document as specified in 3GPP TS 24.481 [31]. The local policy decisions can also include taking into account whether the imminent-peril indicator or emergency indicator was received in the SIP INVITE request.

b) shall return a SIP 486 (Busy Here) response with the warning text set to "122 too many participants" to the originating network as specified in subclause 4.4 Otherwise, continue with the rest of the steps;

11) shall generate a SIP 200 (OK) response as specified in the subclause 6.3.3.2.3.2;

12) 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;

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

NOTE 3: Resulting media plane processing is completed before the next step is performed.

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

15) shall generate a notification to the MCPTT clients, which have subscribed to the conference state event package that the inviting MCPTT User has joined in the MCPTT group session, as specified in subclause 6.3.3.4; and

NOTE 4: As a group document can potentially have a large content, the controlling MCPTT function can notify using content-indirection as defined in IETF RFC 4483 [32].

16) shall send a SIP NOTIFY request to each MCPTT client according to 3GPP TS 24.229 [4].

10.1.1.4.6 Late call entry initiated by controlling MCPTT function

When controlling MCPTT function is notified that an MCPTT client is newly affiliated or comes back from out of coverage, the controlling MCPTT function shall invite the MCPTT client to join an ongoing MCPTT group call by following the procedures specified in subclause 10.1.1.4.1.

NOTE: How the MCPTT function is informed when an MCPTT client is coming back from out of coverage is out of scope of present document.

10.1.1.4.7 Receipt of a SIP re-INVITE request

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.

Upon receipt of a SIP re-INVITE request for an MCPTT session identity identifying an on-demand prearranged MCPTT group session, the controlling 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 re-INVITE request with a SIP 500 (Server Internal Error) response. The controlling 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 skip the rest of the steps;

NOTE 1: If the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "true", the controlling MCPTT function can choose to accept the request.

2) if received SIP re-INVITE request includes an application/vnd.3gpp.mcptt-info+xml MIME body with an <emergency-ind> element included or an <imminentperil-ind> element included, shall validate the request as described in subclause 6.3.3.1.17;

3) if the received SIP re-INVITE request contains an unauthorised request for an MCPTT emergency call as determined by subclause 6.3.3.1.13.2:

a) shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response as specified in subclause 6.3.3.1.14; and

b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

4) if the received SIP re-INVITE request contains an imminent peril indication set to "true" for an MCPTT imminent peril group call and this is an unauthorised request for an MCPTT imminent peril group call as determined by subclause 6.3.3.1.13.6, shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response with the following clarifications:

a) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "false"; and

b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

5) if a Resource-Priority header field is included in the received SIP re-INVITE request:

a) if the Resource-Priority header field is set to the value indicated for emergency calls and the SIP re-INVITE request does not contain an emergency indication and the in-progress emergency state of the group is set to a value of "false", shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response and skip the rest of the steps; and

b) if the Resource-Priority header field is set to the value indicated for imminent peril calls and the SIP re-INVITE request does not contain an imminent peril indication and the in-progress imminent peril state of the group is set to a value of "false", shall reject the SIP INVITE request with a SIP 403 (Forbidden) response and skip the rest of the steps;

6) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "true" and is an authorised request to initiate an MCPTT emergency group call as determined by subclause 6.3.3.1.13.2, the controlling MCPTT function shall:

i) shall cache the MCPTT ID of the MCPTT user that has initiated an MCPTT emergency call;

ii) if the received SIP INVITE contains an alert indication set to a value of "true" and this is an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, shall cache the MCPTT ID of the MCPTT user that has initiated an MCPTT emergency alert;

iii) if the in-progress emergency state of the group is set to a value of "true":

A) for each of the other affiliated member of the group generate a SIP MESSAGE request notification of the MCPTT user's emergency indication as specified in subclause 6.3.3.1.11, setting the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "true";

B) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4]; and

C) if the in-progress imminent peril state of the group is set to a value of "true", shall set it to a value of "false"; and

iv) if the in-progress emergency state of the group is set to a value of "false":

A) shall set the value of the in-progress emergency state of the group to "true";

B) shall start timer TNG2 (in-progress emergency group call timer) and handle its expiry as specified in subclause 6.3.3.1.16;

NOTE 2: The interactions of TNG2 with the TNG3 (group call timer) are explained in subclause 6.3.3.5.2.

C) shall generate SIP re-INVITE requests for the MCPTT emergency group call to the other participants of the MCPTT group call as specified in subclause 6.3.3.1.6;

D) shall send the SIP re-INVITEs towards the other participants of the MCPTT group call; and

E) upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5];

7) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "false" and is an unauthorised request for an MCPTT emergency group call cancellation as determined by subclause 6.3.3.1.13.4:

   a) shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response;

   b) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in annex F.1 with an <emergency-ind> element set to a value of "true";

   c) if an <alert-ind> element of the mcpttinfo MIME body is included in the SIP re-INVITE request set to "false", and there is an outstanding MCPTT emergency alert for the MCPTT user, shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <alert-ind> element set to a value of "true"; and

   d) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

8) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "false" and is determined to be an authorised request for an MCPTT emergency call cancellation as specified in subclause 6.3.3.1.16 and the in-progress emergency state of the group to is set to a value of "true" the controlling MCPTT function:

   a) shall set the in-progress emergency group state of the group to a value of "false";

   b) shall clear the cache of the MCPTT ID of the MCPTT user as having an outstanding MCPTT emergency group call;

   c) if an <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body is included and set to "false" and is determined to be an authorised request for an MCPTT emergency alert cancellation as specified in subclause 6.3.3.1.13.3 and there is an outstanding MCPTT emergency alert for the MCPTT user shall:

      i) if the received SIP re-INVITE request contains an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, clear the cache of the MCPTT ID of the MCPTT user identified by the <originated-by> element as having an outstanding MCPTT emergency alert; or

      ii) if the received SIP re-INVITE request does not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, clear the cache of the MCPTT ID of the sender of the SIP re-INVITE request as having an outstanding MCPTT emergency alert;

   d) shall generate SIP re-INVITE requests to the participants in the group call as specified in subclause 6.3.3.1.6. The MCPTT controlling function:

      i) for each of the other participants in the group call shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

      ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5];

NOTE 3: Subclause 6.3.3.1.6 will inform the group call participants of the cancellation of the MCPTT group's in-progress emergency state and the cancellation of the MCPTT emergency alert if applicable.

   e) shall stop timer TNG2 (in-progress emergency group call timer); and

NOTE 4: The interactions of TNG2 with the TNG3 (group call timer) are explained in subclause 6.3.3.5.2;

   f) for each of the affiliated members of the group that are not participating in the call:

      i) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's emergency call as specified in subclause 6.3.3.1.11;

      ii) set the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false";

      iii) if indicated above in step 8) c), set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false"; and

      iv) send the SIP MESSAGE request according to 3GPP TS 24.229 [4];

9) if the received SIP re-INVITE request contains an imminent peril indication and the in-progress emergency group state of the group is set to a value of "false", shall perform the procedures specified in subclause 10.1.1.4.8 and skip the rest of the steps.

Upon receiving a SIP 200 (OK) response to a SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5];

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

2) shall include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.3.3.2.1;

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

4) shall include the "tdialog" option tag in a Supported header field according to IETF RFC 4538 [23];

5) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "true" and if this is an unauthorised request for an MCPTT emergency alert as determined by subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

6) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "false" and if this is an unauthorised request for an MCPTT emergency alert cancellation as determined by subclause 6.3.3.1.13.3, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

7) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "true", this is an authorised request for an MCPTT imminent peril group call and the in-progress emergency state of the group is set to a value of "true", shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

NOTE 5: In this case, the request was for an imminent peril call but a higher priority MCPTT emergency call was already in progress on the group. Hence, the imminent peril call request aspect of the request is denied but the request is granted with emergency level priority.

8) shall interact with media plane as specified in 3GPP TS 24.380 [5]; and

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

Upon receiving a SIP ACK to the SIP 200 (OK) response sent towards the inviting MCPTT client, and the SIP 200 (OK) response was sent with the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.18.

Upon receipt of a SIP 2xx response for an outgoing SIP MESSAGE request, shall handle according to 3GPP TS 24.229 [4].

10.1.1.4.8 Handling of a SIP re-INVITE request for imminent peril session

This procedure is initiated by the controlling MCPTT function as the result of an action in subclause 10.1.1.4.7.

In the procedures in this subclause:

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

When the controlling function receives a SIP re-INVITE request with an imminent peril indication set to "true", the controlling function:

1) if the in-progress emergency state of the group is set to a value of "false" and if the SIP re-INVITE request contains an imminent peril indication set to a value of "true" or the in-progress imminent peril state of the group to "true", the controlling MCPTT function shall:

NOTE: 1 The calling procedure has already determined that this is not an unauthorised request for an MCPTT imminent peril call, therefore that check does not need to be repeated in the current procedure.

a) if the in-progress imminent peril state of the group is set to a value of "true" and the MCPTT user is indicating a new imminent peril indication:

i) for each of the other affiliated member of the group generate a SIP MESSAGE request notification of the MCPTT user's imminent peril indication as specified in subclause 6.3.3.1.11 with the following clarifications;

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

B) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4];

b) if the in-progress imminent peril state of the group is set to a value of "false";

i) set the value of the in-progress imminent peril state of the group to "true";

ii) generate SIP re-INVITE requests for the MCPTT imminent peril group call to participants in the MCPTT group call as specified in subclause 6.3.3.1.15;

iii) send the SIP re-INVITES to all of the other participants in the MCPTT group call;

iv) for each of the affiliated members of the group not participating in the group call, generate a SIP MESSAGE request notification of the MCPTT user's imminent peril indication as specified in subclause 6.3.3.1.11 with the following clarifications;

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

B) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4]; and

c) cache the information that the MCPTT user has initiated an MCPTT imminent peril call;

2) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "false" and is an unauthorised request for an MCPTT imminent peril group call cancellation as determined by subclause 6.3.3.1.13.6 shall:

a) reject the SIP re-INVITE request with a SIP 403 (Forbidden) response to the SIP re-INVITE request; and

b) include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in Annex F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "false";

c) send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4]; and

d) skip the rest of the steps;

3) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "false" and is determined to be an authorised request for an MCPTT imminent peril call cancellation as specified in subclause 6.3.3.1.13.6 and the in-progress imminent peril state of the group to is set to a value of "true" the controlling MCPTT function shall:

a) set the in-progress imminent peril state of the group to a value of "false";

b) cache the information that the MCPTT user no longer has an outstanding MCPTT imminent peril group call;

c) generate SIP re-INVITES requests to the other participants in the MCPTT group call as specified in subclause 6.3.3.1.15. The MCPTT controlling function:

i) for each participant shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function interact with the media plane as specified in 3GPP TS 24.380 [5]; and

NOTE 2: Subclause 6.3.3.1.15 will inform the affiliated and joined members of the cancellation of the MCPTT group's in-progress emergency state and the cancellation of the MCPTT emergency alert if applicable.

d) for each of the affiliated members of the group not participating in the call shall:

i) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's imminent peril call as specified in subclause 6.3.3.1.11;

ii) set the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false"; and

iii) send the SIP MESSAGE request according to 3GPP TS 24.229 [4];

4) shall include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.3.3.2.1;

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

6) shall include the "tdialog" option tag in a Supported header field according to IETF RFC 4538 [23];

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

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

Upon receipt of a SIP 2xx response for an outgoing SIP MESSAGE request, shall handle according to 3GPP TS 24.229 [4].

10.1.1.5 Non-controlling function of an MCPTT group procedures

10.1.1.5.1 Originating procedures

This subclause describes the procedures for inviting an MCPTT user to an MCPTT session. The procedure is initiated by the non-controlling MCPTT function of an MCPTT group as the result of an action in subclause 10.1.1.5.2 or subclause 10.1.1.5.5.

The non-controlling MCPTT function:

1) shall invite the MCPTT clients as specified in subclause 6.3.4.1.2;

2) shall include in each SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request from the controlling MCPTT function according to the procedures specified in subclause 6.3.4.1.1; and

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

For each SIP 183 (Session Progress) response received to each SIP INVITE request sent to an MCPTT client, the non-controlling MCPTT function of an MCPTT group:

1) For each SIP 183 (Session Progress) response containing the option tag "100rel", shall send a SIP PRACK request towards the MCPTT client according to 3GPP TS 24.229 [4]; and

2) shall cache the received response;

For each SIP 200 (OK) response received to each SIP INVITE request sent to an MCPTT client, the non-controlling MCPTT function of an MCPTT group:

1) shall send a SIP ACK request towards the MCPTT client according to 3GPP TS 24.229 [4];

2) shall cache the SIP 200 (OK) response;

3) shall start the SIP session timer according to rules and procedures of IETF RFC 4028 [7]; and

4) if at least one of the participants has subscribed to the conference event package, shall send a SIP NOTIFY request to all participants with a subscription to the conference event package as specified in subclause 10.1.3.5.2.

On receipt of a SIP 3xx, 4xx, 5xx or 6xx response from an invited MCPTT client, the non-controlling MCPTT function of an MCPTT group:

1) shall send an SIP ACK request towards the MCPTT client as specified in 3GPP TS 24.229 [4];

2) shall remove the cached provisional responses received from the MCPTT client, if any cached provisional responses exists; and

3) if the procedures are initiated by the receipt of the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" as specified in subclause 10.1.1.5.2, shall cache the SIP 3xx, 4xx, 5xx or 6xx response.

10.1.1.5.2 Terminating procedures

10.1.1.5.2.1 General

When receiving the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" the MCPTT server can be acting as a controller MCPTT function in an ongoing prearranged group call or, if an prearranged group call is not ongoing, be initiated as an non-controlling MCPTT function and invite MCPTT users.

If a prearranged group call is not ongoing the MCPTT server shall perform the actions specified in subclause 10.1.1.5.2.2.

If the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" is received when a prearranged group call is ongoing, the controlling MCPTT function may switch from operating in a controlling MCPTT function mode to operate in a non-controlling MCPTT function mode as specified in subclause 10.1.1.5.2.3.

When operating in the non-controlling mode and a SIP BYE request is received from the controlling MCPTT function, the non-controlling MCPTT function shall change from operating in the non-controlling mode to operating in the controlling mode as specified in subclause 10.1.1.5.2.4.

10.1.1.5.2.2 Initiating a prearranged group call

Upon receipt of a "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" and if a prearranged group call is not ongoing, the non-controlling MCPTT function of an MCPTT group:

NOTE 1: The Contact header field of the SIP INVITE request contains the "isfocus" feature media tag.

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 controlling 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;

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. Otherwise, continue with the rest of the steps;

3) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

4) if the partner MCPTT system does not have a mutual aid relationship with the primary MCPTT system identified by the contents of the P-Asserted-Identity, shall reject the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" with a SIP 403 (Forbidden) response, with warning text set to "128 isfocus already assigned" in a Warning header field as specified in subclause 4.4, and shall not process the remaining steps;

5) if a trusted mutual aid relationship exists between the partner MCPTT system and the primary MCPTT system and the procedure in 3GPP TS 23.379 [3] subclause 10.6.2.4.2 is supported:

   a) shall generate a SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4];

   b) shall retrieve the group members of the prearranged group identified by the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request, as specified in subclause 6.3.5.2;

c) if the retrieval of group members was successful shall include a P-Refused-URI-List header field populated with affiliated members of the prearranged group in accordance with the IETF RFC 5318 [36]:

d) if the retrieval of group members was not successful, shall include the warning text set to "128 isfocus already assigned" in a Warning header field as specified in subclause 4.4; and

e) shall send the SIP 403 (Forbidden) response towards the controlling MCPTT function as specified in 3GPP TS 24.229 [4]; and

f) shall not process the remaining steps;

6) shall retrieve the group document from the group management server for the MCPTT group ID contained in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request and carry out initial processing as specified in subclause 6.3.5.2 and continue with the rest of the steps if the checks in subclause 6.3.5.2 succeed;

7) shall cache the content of the SIP INVITE request, if received in the Contact header field and if the specific feature tags are supported;

8) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

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

10) if the group document retrieved from the group management server contains <on-network-required> group members as specified in 3GPP TS 24.481 [31], shall send a SIP 183 (Session Progress) response to the SIP INVITE request for non-controlling MCPTT function of an MCPTT group as specified in subclause 6.3.4.2.2.1 and shall populate the response with an application/vnd.3gpp.mcptt-info+xml MIME body containing the <required> element set to "true".

11) if the group document retrieved from the group management server does not contain any <on-network-required> group members as specified in 3GPP TS 24.481 [31], may, according to local policy, send a SIP 183 (Session Progress) response to the SIP INVITE request for non-controlling MCPTT function of an MCPTT group as specified in subclause 6.3.4.2.2.1;

12) shall invite each group member determined in step 9) above, to the group session, as specified in subclause 10.1.1.5.1; and

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

Unless a SIP response has been sent to the controlling MCPTT function as specified in step 10 or 11 above, the non-controlling MCPTT function of an MCPTT group shall wait for the first SIP provisional response or first SIP 200 (OK) response from one of the invited MCPTT clients, before sending a response to the SIP INVITE request for non-controlling MCPTT function of an MCPTT group.

Upon receiving the first 18x response to a SIP INVITE request sent to an invited MCPTT client as specified in subclause 10.1.1.5.1, not containing a P-Answer-State header field, and if a SIP 183 (Session Progress) response has not already been sent in response to the SIP INVITE request for non-controlling MCPTT function of an MCPTT group, the non-controlling MCPTT function of an MCPTT group:

1) shall generate a SIP 183 (Session Progress) response as described in subclause 6.3.4.2.2.1; and

2) shall forward the SIP 183 (Session Progress) response to the controlling MCPTT function according to 3GPP TS 24.229 [4].

Upon receiving the first 18x response to a SIP INVITE request sent to an invited MCPTT client as specified in subclause 10.1.1.5.1, containing a P-Answer-State header field with the value "Unconfirmed" as specified in IETF RFC 4964 [34], a SIP 183 (Session Progress) response has not already been sent in response to the SIP INVITE request for non-controlling MCPTT function of an MCPTT group and the non-controlling MCPTT function of an MCPTT group supports media buffering, the non-controlling MCPTT function of an MCPTT group:

1) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.4.2.2.2 before continuing with the rest of the steps;

2) 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 6.3.4.2.1;

3) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3.5; and

NOTE 2: Resulting media plane processing is completed before the next step is performed.

4) shall send a SIP 200 (OK) response to the controlling MCPTT function according to 3GPP TS 24.229 [4].

If the group document does not contain any <on-network-required> group members as specified in 3GPP TS 24.481 [31], then upon receiving the first SIP 200 (OK) response to a SIP INVITE request sent to an invited MCPTT client as specified in subclause 10.1.1.5.1, the non-controlling MCPTT function of an MCPTT group:

1) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.4.2.2.2 before continuing with the rest of the steps;

2) 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 6.3.4.2.1;

3) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3.5; and

NOTE 3: Resulting media plane processing is completed before the next step is performed.

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

If the group document contains <on-network-required> group member(s) as specified in 3GPP TS 24.481 [31], then the non-controlling MCPTT function of an MCPTT group shall wait until all SIP 200 (OK) responses to SIP INVITE requests have been received from the <on-network-required> MCPTT clients before sending a SIP 200 (OK) response back to the controlling MCPTT function, as specified above.

If all invited MCPTT clients have rejected SIP INVITE requests with a SIP 3xx, 4xx, 5xx or 6xx response, the non-controlling MCPTT function of an MCPTT group:

1) shall generate a SIP reject response as specified in 3GPP TS 24.229 [4];

2) shall, from the list of reject response codes cached by the non-controlling MCPTT function of an MCPTT group, select the highest prioritized cached reject response code as specified in IETF RFC 3261 [24]; and

3) shall send the reject response towards the controlling MCPTT function as specified in 3GPP TS 24.229 [4].

10.1.1.5.2.3 Joining an ongoing prearranged group call

Upon receipt of a "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" and if a prearranged group call is already ongoing, the non-controlling MCPTT function of an MCPTT group:

NOTE 1: The Contact header field of the SIP INVITE request contains the "isfocus" feature media tag.

1) 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. Otherwise, continue with the rest of the steps;

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

3) if the partner MCPTT system does not have a mutual aid relationship to merged an ongoing prearranged call with the primary MCPTT system identified by the contents of the P-Asserted-Identity, shall reject the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" with a SIP 403 (Forbidden) response, with warning text set to "128 isfocus already assigned" in a Warning header field as specified in subclause 4.4, and shall not process the remaining steps;

4) shall cache the content of the SIP INVITE request, if received in the Contact header field and if the specific feature tags are supported;

5) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

6) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.4.2.2.2 before continuing with the rest of the steps;

7) 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 6.3.4.2.1;

8) shall instruct the media plane to initialise the switch to non-controlling mode as specified in 3GPP TS 24.380 [5] subclause 6.5.2.3;

NOTE 2: Resulting media plane processing is completed before the next step is performed. The media plane indicates the state of the floor and if the state is "floor-taken", information about the current speaker.

9) if the media plane provided information about the current speaker, cache the information about the current speaker(s);

10) shall send a SIP 200 (OK) response to the controlling MCPTT function according to 3GPP TS 24.229 [4].

Upon receipt of the SIP ACK request, the non-controlling MCPTT function of an MCPTT group:

1) if information about a current speaker is cached:

   a) shall generate a SIP INFO request as specified in subclause 6.3.4.1.3; and

   b) shall send the SIP INFO request to the controlling MCPTT function as specified in 3GPP TS 24.229 [4];

2) shall instruct the media plane to finalise the switch to the non-controlling mode as specified in 3GPP TS 24.380 [5] subclause 6.3.5.3; and

3) if at least one of the MCPTT clients in the pre-arranged group session has a subscription to the conference event package, shall subscribe to the conference event package from the controlling MCPTT function as specified in subclause 10.1.3.5.3.

10.1.1.5.2.4 Splitting an ongoing prearranged group call

Upon receipt of a SIP BYE request or a final SIP reject response from the controlling MCPTT function, the non-controlling MCPTT function of an MCPTT group:

1) if keeping the prearranged group call active is according to the release policy in subclause 6.3.8.1, shall request media plane to switch to controlling mode as specified in 3GPP TS 24.380 [5] subclause 6.3.5;

NOTE 1: Resulting media plane processing is completed before the next step is performed.

2) if a SIP BYE request was received, shall send a SIP 200 (OK) response to the SIP BYE request; and

3) if keeping the prearranged group call active is according to the release policy in subclause 6.3.8.1 and if at least one of the remaining MCPTT clients has subscribed to the conference package, shall send a NOTIFY request to all participants with a subscription to the conference event package as specified in subclause 10.1.3.5.2.

NOTE 2: The SIP NOTIFY request will indicate that all participants, with the exception of the MCPTT users belonging to the constituent MCPTT group hosted by the non-controlling MCPTT function, have left the group session.

10.1.1.5.3 Rejoin procedures

10.1.1.5.3.1 Terminating procedures

Upon receipt of a SIP INVITE request that includes an MCPTT session identity of an ongoing MCPTT session in the Request-URI the non-controlling MCPTT function act as a controlling MCPTT function towards the MCPTT client and shall perform the actions in the subclause 10.1.1.4.5.1 with the following clarifications:

1) the MCPTT session identity in the Contact header field of the SIP 200 (OK) response shall be the MCPTT session identity generated by the non-controlling MCPTT function; and

2) the subclause 10.1.3.5.2 shall be used when sending the SIP NOTIFY request for subscriptions to the conference event package.

10.1.1.5.3.2 Late call entry initiated by non-controlling MCPTT function

When non-controlling MCPTT function is notified that an MCPTT client is newly affiliated or comes back from out of coverage, the non-controlling MCPTT function shall invite the MCPTT client to join an ongoing MCPTT group call by following the procedures specified in subclause 10.1.1.5.1.

NOTE: How the MCPTT function is informed when an MCPTT client is coming back from out of coverage is out of scope of present document.

10.1.1.5.4 SIP OPTIONS request authorization procedure

Upon receipt of an SIP OPTIONS request containing a P-Asserted-Identity header field containing the public service identity of a MCPTT server not authorized to send the SIP OPTIONS request, the non-controlling MCPTT function of an MCPTT group shall send a SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 and exit this subclause.

Upon receipt of an SIP OPTIONS request containing a P-Asserted-Identity header field containing the public service identity of a MCPTT server authorized to send the SIP OPTIONS request, the non-controlling MCPTT function of an MCPTT group shall perform the actions in this subclause.

The non-controlling MCPTT function shall retrieve the group document from the group management server for the MCPTT group ID contained in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP OPTIONS request with the following clarifications:

NOTE: The action of the non-controlling MCPTT function of an MCPTT group on receipt of the SIP OPTIONS request mimics the actions of the non-controlling MCPTT function of an MCPTT group on receipt of the SIP INVITE request.

The non-controlling MCPTT function shall:

1) if the non-controlling MCPTT function fails to retrieve the group document from the group management server, send a shall send the SIP 404 (Not Found) response to the SIP OPTIONS request with the warning text set to "113 group document does not exist" in a Warning header field as specified in subclause 4.4;

2) if the non-controlling MCPTT function successfully retrieves the group document from the group management server or if the group document was already cached and if one of the following conditions are fulfilled:

   a) if the constituent MCPTT group is a chat group and the rules for joining a group conference as specified in subclause 6.3.5.3 are fulfilled; or

   b) if the constituent MCPTT group is a prearranged group and the rules for initiating a prearranged group session as specified in subclause 6.3.5.4;

   then the non-controlling MCPTT function:

   a) shall send the SIP 200 (OK) response to the SIP OTIONS response as specified in 3GPP TS 24.229 [4] and the IETF RFC 3261 [24] populated as follows:

      i) shall include a warning text set to "147 user is authorized to initiate a temporary group call" in a Warning header field as specified in subclause 4.4;

      ii) shall include an application/vnd.3gpp.mcptt-info MIME body with:

         A) the <session-type> element set to "chat", if the constituent MCPTT group is a chat group; and

         B) the <session-type> element set to "prearranged", if the constituent MCPTT group is a prearranged group; and

      iii) shall include the P-Asserted-Identity of the non-controlling MCPTT function of an MCPTT group; and

3) if none of the conditions in step 2 above) are fulfilled, shall send a SIP 403 (Forbidden) response with the warning text set to "119 user is not authorised to initiate the group call" in a Warning header field as specified in subclause 4.4.

10.1.1.5.5 Initiating a temporary group session

Upon receiving a "SIP INVITE request for controlling MCPTT function of an MCPTT group" when a prearranged group session is not ongoing, the non-controlling MCPTT-function shall:

NOTE 1: The difference between a "SIP INVITE request for controlling MCPTT function of an MCPTT group" and a "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" is that the latter SIP INVITE request contains the isfocus media feature tag in the Contact header field.

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 non-controlling 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;

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. Otherwise, continue with the rest of the steps;

3) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

4) shall retrieve the group document from the group management server for the MCPTT group ID contained in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request and carry out initial processing as specified in subclause 6.3.5.2 and continue with the rest of the steps if the checks in subclause 6.3.5.2 succeed;

NOTE 2: If the checks are not succesful, the SIP response to the "SIP INVITE request for controlling MCPTT function of an MCPTT group" is already sent in the subclause 6.3.5.2.

5) shall cache the content of the SIP INVITE request;

6) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

7) shall authorize the MCPTT user in the <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the "SIP INVITE request for controlling MCPTT function of an MCPTT group" as specified in subclause 6.3.5.4, if the MCPTT user is unauthorized to initiated a pre-arranged group session the non-controlling MCPTT function shall send a SIP 403 (Forbidden) response with the warning text set to "119 user is not authorised to initiate the group call" in a Warning header field as specified in subclause 4.4.

8) shall generate a SIP INVITE request to the controlling MCPTT function as specified in subclause 6.3.4.1.4; and

9) shall send the SIP INVITE request to the controlling MCPTT function as specified in 3GPP TS 24.229 [4].

Upon receipt of a SIP 2xx response to the SIP INVITE request sent to the controlling MCPTT function as specified above, the non-controlling MCPTT function:

1) shall send the SIP ACK request to the controlling MCPTT function as specified in 3GPP TS 24.229 [4];

2) shall generate a SIP 200 (OK) to the "SIP INVITE request for controlling MCPTT function of an MCPTT group" as specified in 3GPP TS 24.229 populated as follows:

   a) shall include an SDP answer as specified in subclause 6.3.4.2.1 based on the SDP answer in the SIP 200 (OK) response;

   b) shall include the public service identifier of the non-controlling MCPTT function in the P-Asserted-Identity header field;

   c) shall include the warning text set to "148 MCPTT group is regrouped" in a Warning header field as specified in subclause 4.4; and

   d) shall send the SIP 200 (OK) request according to 3GPP TS 24.229;

NOTE 3: As long as the MCPTT group is regrouped the floor control messages in the media plane includes a grouped regrouped indication as specified in 3GPP TS 24.380 [5].

3) shall start acting as a non-controlling MCPTT function and interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.5;

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

5) shall invite each group member determined in step 4) immediately above, to the group session, as specified in subclause 10.1.1.5.1.

Upon receipt of other final SIP responses with the exception of the SIP 2xx response to the INVITE request sent to the controlling MCPTT function as specified above, the non-controlling MCPTT function:

1) shall send the SIP ACK response to the controlling MCPTT function as specified in 3GPP TS 24.229 [4]; and

2) shall start acting as a controlling MCPTT function as specified in subclause 10.1.1.4 and invite members as specified in subclause 6.3.4.1.2.

NOTE 4: Regardless if the controlling MCPTT function accepts or rejects the SIP INVITE request sent above the prearranged group session continues to be initiated with only the members of the group homed on the non-controlling MCPTT function of the group being invited to the group call.

The non-controlling MCPTT function shall handle SIP responses (other than the SIP 2xx response) to the SIP INVITE requests sent to invited members as specified in 3GPP TS 24.229.

Upon receipt of a SIP 2xx response to SIP INVITE requests sent to invited members, the non-controlling MCPTT function:

1) shall send the SIP ACK request as specified in 3GPP TS 24.229 [4]; and

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

10.1.2 Chat group (restricted) call

10.1.2.1 General

10.1.2.2 MCPTT client procedures

10.1.2.2.1 On-demand chat group call

10.1.2.2.1.1 Procedure for initiating a chat MCPTT group session and procedure for joining a chat MCPTT group session

Upon receiving a request from an MCPTT user to initiate or join an MCPTT group session using an MCPTT group identity, identifying a chat MCPTT group, the MCPTT client shall generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) if the MCPTT user has requested the origination of an MCPTT emergency group call or is originating an MCPTT chat group call and the MCPTT emergency state is already set, the MCPTT client shall comply with the procedures in subclause 6.2.8.1.1;

2) if the MCPTT user has requested the origination of an MCPTT imminent peril group call, the MCPTT client shall comply with the procedures in subclause 6.2.8.1.9;

3) shall include the g.3gpp.mcptt media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

4) 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];

5) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP INVITE request;

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

7) should include the "timer" option tag in the Supported header field;

8) should include the Session-Expires header field according to IETF RFC 4028 [7]. It is recommended that the refresher parameter is omitted. If included, the refresher parameter shall be set to "uac";

9) shall set the Request-URI of the SIP INVITE request to the public service identity identifying the participating MCPTT function serving the MCPTT user;

NOTE 1: The MCPTT client is configured with public service identity identifying the participating MCPTT function serving the MCPTT user.

10) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [4];

11) if the MCPTT client emergency group state for this group is set to "MEG 2: in-progress" or "MEG 4: confirm-pending", the MCPTT client shall comply with the procedures in subclause 6.2.8.1.2;

12) if the MCPTT client imminent peril group state for this group is set to "MIG 2: in-progress" or "MIG 4: confirm-pending" shall include the Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.12;

13) shall contain an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with:

   a) the <session-type> element set to a value of "chat";

   b) the <mcptt-request-uri> element set to the group identity; and

   c) the <mcptt-client-id> element set to the MCPTT client ID of the originating MCPTT client;

NOTE 2: The MCPTT ID of the originating MCPTT user is not included in the body, as this will be inserted into the body of the SIP INVITE request that is sent by the originating participating MCPTT function.

14) shall include in the SIP INVITE request an SDP offer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.2.1;

15) if an implicit floor request is required, shall indicate this as specified in subclause 6.4; and

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

On receiving a SIP 2xx response to the SIP INVITE request, the MCPTT client:

1) shall interact with the user plane as specified in 3GPP TS 24.380 [5]; and

2) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested" or "MEGC 3: emergency-call-granted" or the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted", the MCPTT client shall perform the actions specified in subclause 6.2.8.1.4.

On receiving a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request:

1) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested" or "MEGC 3: emergency-call-granted"; or

2) if the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted";

the MCPTT client shall perform the actions specified in subclause 6.2.8.1.5.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.1.13.

10.1.2.2.1.2 MCPTT client receives SIP re-INVITE request

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

Upon receipt of a SIP re-INVITE request the MCPTT client:

1) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "true":

   a) should display to the MCPTT user the MCPTT ID of the originator of the MCPTT emergency group call and an indication that this is an MCPTT emergency group call;

   b) if the <mcpttinfo> element containing the <mcptt-Params> element contains an <alert-ind> element set to "true", should display to the MCPTT user an indication of the MCPTT emergency alert and associated information;

   c) shall set the MCPTT emergency group state to "MEG 2: in-progress";

   d) shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril";and

   e) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-gc-capable";

2) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "true":

   a) should display to the MCPTT user the MCPTT ID of the originator of the MCPTT imminent peril group call and an indication that this is an MCPTT imminent peril group call; and

   b) shall set the MCPTT imminent peril group state to "MIG 2: in-progress";

3) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "false":

   a) should display to the MCPTT user the MCPTT ID of the MCPTT user cancelling the MCPTT emergency group call;

   b) if the <mcpttinfo> element containing the <mcptt-Params> element contains an <alert-ind> element set to "false":

      i) should display to the MCPTT user an indication of the MCPTT emergency alert cancellation and the MCPTT ID of the MCPTT user cancelling the MCPTT emergency alert; and

      ii) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body including an <originated-by> element:

         A) should display to the MCPTT user the MCPTT ID contained in the <originated-by> element of the MCPTT user that originated the MCPTT emergency alert; and

         B) if the MCPTT ID contained in the <originated-by> element is the MCPTT ID of the receiving MCPTT user, shall set the MCPTT emergency alert state to "MEA 1: no-alert";

   c) shall set the MCPTT emergency group state to "MEG 1: no-emergency"; and

   d) if the MCPTT emergency group call state of the group is set to "MEGC 3: emergency-call-granted", shall set the MCPTT emergency group call state of the group to "MEGC 1: emergency-gc-capable";

4) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "false":

   a) should display to the MCPTT user the MCPTT ID of the MCPTT user cancelling the MCPTT imminent peril group call and an indication that this is an MCPTT imminent peril group call;

   b) shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; and

   c) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-gc-capable";

5) may check if a Resource-Priority header field is included in the incoming SIP re-INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

6) shall accept the SIP re-INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [4];

7) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP 200 (OK) response;

8) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP 200 (OK) response;

9) if the SIP re-INVITE request was received within an on-demand session, shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP re-INVITE request according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.2;

10) if the SIP re-INVITE request was received within a pre-established session, shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session; and

NOTE: The SIP re-INVITE request can be received within an on-demand session or a pre-established session associated with an MCPTT group session. If the SIP re-INVITE request is received within a pre-established session, the media-level section for the MCPTT speech media stream and the media-level section of the media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

11) shall send the SIP 200 (OK) response towards the MCPTT server according to rules and procedures of 3GPP TS 24.229 [4].

10.1.2.2.1.3 MCPTT in-progress emergency cancel

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

Upon receiving a request from an MCPTT user to cancel the in-progress emergency condition on a chat MCPTT group, the MCPTT client shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) if the MCPTT user is not authorised to cancel the in-progress emergency group state of the MCPTT group as determined by the procedures of subclause 6.2.8.1.7, the MCPTT client:

   a) should indicate to the MCPTT user that they are not authorised to cancel the in-progress emergency group state of the MCPTT group; and

   b) shall skip the remaining steps of the current subclause;

2) shall, if the MCPTT user is cancelling an in-progress emergency condition and optionally an MCPTT emergency alert originated by the MCPTT user, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.3;

3) shall, if the MCPTT user is cancelling an in-progress emergency condition and optionally an MCPTT emergency alert originated by another MCPTT user, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.14;

4) shall, if the SIP re-INVITE request is to be sent within an on-demand session, include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.2.1;

5) if the SIP re-INVITE request is to be sent within a pre-established session, shall include an SDP offer in the SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session;

NOTE 1: The SIP re-INVITE request can be sent within an on-demand session or a pre-established session associated with an MCPTT group session. If the SIP re-INVITE request is sent within a pre-established session, the media-level section for the MCPTT speech media stream and the media-level section of the media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

6) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.2; and

7) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP re-INVITE request, the MCPTT client:

1) shall set the MCPTT emergency group state of the group to "MEG 1: no-emergency";

2) shall set the MCPTT emergency group call state of the group to "MEGC 1: emergency-gc-capable"; and

3) if the MCPTT emergency alert state is set to "MEA 4: Emergency-alert-cancel-pending", the sent SIP re-INVITE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body and the SIP 2xx response to the SIP request for a priority group call does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", shall set the MCPTT emergency alert state to "MEA 1: no-alert".

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request:

1) shall set the MCPTT emergency group state as "MEG 2: in-progress";

2) if the SIP 4xx response, SIP 5xx response or SIP 6xx response contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to a value of "true" and the sent SIP re-INVITE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated"; and

3) if the SIP 4xx response, SIP 5xx response or SIP 6xx response did not contain an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element and did not contain an <originated-by> element, the MCPTT emergency alert (MEA) state shall revert to its value prior to entering the current procedure.

NOTE 3: If the in-progress emergency group state cancel request is rejected, the state of the session does not change, i.e. continues with MCPTT emergency group call level priority.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.1.13.

10.1.2.2.1.4 MCPTT upgrade to in-progress emergency or imminent peril

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

Upon receiving a request from an MCPTT user to upgrade the MCPTT group session to an emergency condition or an imminent peril condition on a chat MCPTT group, the MCPTT client shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [4], with the clarifications given below.

1) if the MCPTT user is requesting to upgrade the MCPTT group session to an in-progress emergency group state and is not authorised to do so as determined by the procedures of subclause 6.2.8.1.8, the MCPTT client:

   a) should indicate to the MCPTT user that they are not authorised to upgrade the MCPTT group session to an in-progress emergency group state; and

   b) shall skip the remaining steps of the current subclause;

2) if the MCPTT user is requesting to upgrade the MCPTT group session to an in-progress imminent peril state and is not authorised to do so as determined by the procedures of subclause 6.2.8.1.8, the MCPTT client:

a) should indicate to the MCPTT user that they are not authorised to upgrade the MCPTT group session to an in-progress imminent peril group state; and

b) shall skip the remaining steps of the current subclause;

3) if the MCPTT user has requested to upgrade the MCPTT group session to an MCPTT emergency call, the MCPTT client:

a) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.1; and

b) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.2.

4) if the MCPTT user has requested to upgrade the MCPTT group session to an MCPTT imminent peril call, the MCPTT client:

a) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.9; and

b) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.12;

5) if the SIP re-INVITE request is to be sent within an on-demand session, shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.2.1;

6) if the SIP re-INVITE request is to be sent within a pre-established session, shall include an SDP offer in the SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session;

NOTE: The SIP re-INVITE request can be sent within an on-demand session or a pre-established session associated with an MCPTT group session. If the SIP re-INVITE request is sent within a pre-established session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

7) if an implicit floor request is required, shall indicate this as specified in subclause 6.4;

8) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.2; and

9) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP re-INVITE request the MCPTT client:

1) shall interact with the user plane as specified in 3GPP TS 24.380 [5]; and

2) shall perform the actions specified in subclause 6.2.8.1.4.

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request the MCPTT client shall perform the actions specified in subclause 6.2.8.1.5.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.1.13.

10.1.2.2.1.5 MCPTT in-progress imminent peril cancel

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

Upon receiving a request from an MCPTT user to cancel the in-progress imminent peril condition on a chat MCPTT group, the MCPTT client shall generate a SIP re-INVITE request by following the procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) if the MCPTT user is not authorised to cancel the in-progress imminent peril group state of the MCPTT group as determined by the procedures of subclause 6.2.8.1.10, the MCPTT client:

a) should indicate to the MCPTT user that they are not authorised to cancel the in-progress imminent peril group state of the MCPTT group; and

b) shall skip the remaining steps of the current subclause;

2) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.1.11;

3) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.12;

4) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with:

a) the <session-type> element set to a value of "chat"; and

b) the <mcptt-request-uri> element set to the group identity;

NOTE 1: The MCPTT ID of the originating MCPTT user is not included in the body, as this will be inserted into the body of the SIP re-INVITE request that is sent by the originating participating MCPTT function.

5) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP re-INVITE request according to IETF RFC 3840 [16];

6) if the SIP re-INVITE request is to be sent within an on-demand session, shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.2.1;

7) if the SIP re-INVITE request is to be sent within a pre-established session, shall include an SDP offer in the SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session; and

NOTE 2: The SIP re-INVITE request can be sent within an on-demand session or a pre-established session associated with an MCPTT group session. If the SIP re-INVITE request is sent within a pre-established session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

8) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP re-INVITE request, the MCPTT client:

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

2) shall set the MCPTT imminent peril group state of the group to "MIG 1: no-imminent-peril"; and

3) shall set the MCPTT imminent peril group call state of the group to "MIGC 1: imminent-peril-gc-capable".

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request:

1) if the SIP 4xx response, SIP 5xx response or SIP 6xx response:

a) contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <imminentperil-ind> element set to a value of "true"; or

b) does not contain an application/vnd.3gpp.mcptt-info+xml MIME body with an <imminentperil-ind> element;

then the MCPTT client shall set the MCPTT imminent peril group state as "MIG 2: in-progress".

NOTE 2: This is the case where the MCPTT client requested the cancellation of the MCPTT imminent peril in-progress state and was rejected.

10.1.2.2.1.6 MCPTT client receives a SIP INVITE request for an MCPTT group call

This procedure is used for MCPTT emergency and MCPTT imminent peril calls when the MCPTT client is affiliated but not joined to the chat group.

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.

Upon receipt of an initial SIP INVITE request, the MCPTT client:

1) may reject the SIP INVITE request if either of the following conditions is met:

   a) MCPTT client does not have enough resources to handle the call; or

   b) any other reason outside the scope of this specification;

2) if the SIP INVITE request is rejected in step 1), shall respond toward participating MCPTT function either with appropriate reject code as specified in 3GPP TS 24.229 [4] and warning texts as specified in subclause 4.4.2 or with SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure and skip the rest of the steps of this subclause;

NOTE 1: if the SIP INVITE request contains an emergency indication or imminent peril indication, the MCPTT client can by means beyond the scope of this specification choose to accept the request.

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

   a) should display to the MCPTT user an indication that this is a SIP INVITE request for an MCPTT emergency group call and:

      i) should display the MCPTT ID of the originator of the MCPTT emergency group call contained in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body;

      ii) should display the MCPTT group identity of the group with the emergency condition contained in the <mcptt-calling-group-id> element; and

      iii) if the <alert-ind> element is set to "true", should display to the MCPTT user an indication of the MCPTT emergency alert and associated information;

   b) shall set the MCPTT emergency group state to "MEG 2: in-progress";

   c) shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; and

   d) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-gc-capable"; otherwise

4) if the SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "true":

   a) should display to the MCPTT user an indication that this is a SIP INVITE request for an MCPTT imminent peril group call and:

      i) should display the MCPTT ID of the originator of the MCPTT imminent peril group call contained in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

      ii) should display the MCPTT group identity of the group with the imminent peril condition contained in the <mcptt-calling-group-id> element; and

   b) shall set the MCPTT imminent peril group state to "MIG 2: in-progress";

5) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

6) shall accept the SIP INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [4];

7) shall include the option tag "timer" in a Require header field of the SIP 200 (OK) response;

8) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP 200 (OK) response;

9) shall include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP 200 (OK) response;

10) shall include the Session-Expires header field in the SIP 200 (OK) response and start the SIP session timer according to IETF RFC 4028 [7]. If no "refresher" parameter was included in the received SIP INVITE request the "refresher" parameter in the Session-Expires header field shall be set to "uas", otherwise shall include a "refresher" parameter set to the value received in the Session-Expires header field the received SIP INVITE request;

11) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP INVITE request according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.2;

12) shall send the SIP 200 (OK) response towards the MCPTT server according to rules and procedures of 3GPP TS 24.229 [4]; and

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

10.1.2.2.2 Chat group call within a pre-established session

10.1.2.2.2.1 Procedure for initiating a chat MCPTT group session and procedure for joining a chat MCPTT group session

Upon receiving a request from an MCPTT user to initiate or join an MCPTT group session using an MCPTT group identity identifying a chat MCPTT group within the pre-established session, the MCPTT client shall generate a SIP REFER request as specified in IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27], and in accordance with the UE procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) shall set the Request URI of the SIP REFER request to the session identity of the pre-established session;

2) shall set the Refer-To header field of the SIP REFER request as specified in IETF RFC 3515 [25] with a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [20], and with the Content-ID header field set to this "cid" URL;

3) shall include in the application/resource-lists MIME body a single <entry> element containing a "uri" attribute set to the chat group identity, extended with the following URI header fields:

NOTE: Characters that are not formatted as ASCII characters are escaped in the following URI header fields;

   a) the 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];

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

   c) an hname "body" URI header field populated with:

      i) an application/sdp MIME body containing an SDP offer, if the session parameters of the pre-established session require modification or if implicit floor control is required, according to the conditions specified in subclause 6.4; and

      ii) an application/vnd.3gpp.mcptt-info MIME body with:

         A) the <session-type> element set to a value of "chat"; and

         B) the <mcptt-client-id> element set to the MCPTT client ID of the originating MCPTT client;

4) if the MCPTT user has requested the origination of an MCPTT emergency group call or is originating an MCPTT group call and the MCPTT emergency state is already set:

   a) if this is an authorised request for an MCPTT emergency group call as determined by the procedures of subclause 6.2.8.8.1.8, shall comply with the procedures in subclause 6.2.8.1.1; and

b) if this is an unauthorised request for an MCPTT emergency group call as determined in step a) above, should indicate to the MCPTT user that they are not authorised to initiate an MCPTT emergency group call;

5) if the MCPTT client emergency group state for this group is set to "MEG 2: in-progress" or "MEG 4: confirm-pending", shall include the Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.2;

6) if the MCPTT user has requested the origination of an MCPTT imminent peril group call:

a) if this is an authorised request for an MCPTT imminent peril group call as determined by the procedures of subclause 6.2.8.8.1.8, shall comply with the procedures in subclause 6.2.8.1.9;

b) if this is an unauthorised request for an MCPTT imminent peril group call as determined in step a) above, should indicate to the MCPTT user that they are not authorised to initiate an MCPTT imminent peril group call;

7) if the MCPTT client imminent peril group state for this group is set to "MIG 2: in-progress" or "MIG 4: confirm-pending" shall include the Resource-Priority header field and comply with the procedures in subclause 6.2.8.1.12;

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

9) shall include the following according to IETF RFC 4488 [22]:

a) the option tag "norefersub" in the Supported header field; and

b) the value "false" in the Refer-Sub header field.

10) shall include a Target-Dialog header field as specified in IETF RFC 4538 [23] identifying the pre-established session;

11) shall include the g.3gpp.mcptt media feature tag in the Contact header field of the SIP REFER request according to IETF RFC 3840 [16]; and

12) shall send the SIP REFER request according to 3GPP TS 24.229 [4].

On receiving a final SIP 2xx response to the SIP REFER request, the MCPTT client:

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

On receiving a SIP 4xx response, SIP 5xx response or a SIP 6xx response to the SIP REFER request:

1) if the MCPTT emergency group call state is set to "MEGC 2: emergency-call-requested" or "MEGC 3: emergency-call-granted"; or

2) if the MCPTT imminent peril group call state is set to "MIGC 2: imminent-peril-call-requested" or "MIGC 3: imminent-peril-call-granted";

the MCPTT client shall perform the actions specified in subclause 6.2.8.1.5 and shall skip the remaining steps.

On receiving a SIP re-INVITE request within the pre-established session targeted by the sent SIP REFER request, and if the sent SIP REFER request was a request for an MCPTT emergency group call or an MCPTT imminent peril group call, the MCPTT client:

1) shall perform the actions specified in subclause 6.2.8.1.16;

2) shall check if a Resource-Priority header field is included in the incoming SIP re-INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

3) shall accept the SIP re-INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [4];

4) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session; and

5) shall send the SIP 200 (OK) response towards the participating MCPTT function according to rules and procedures of 3GPP TS 24.229 [4].

On call release by interaction with the media plane as specified in subclause 9.2.2 of 3GPP TS 24.380 [5] if the sent SIP REFER request was a request for an MCPTT emergency group call or an MCPTT imminent peril group call, the MCPTT client shall perform the procedures specified in subclause 6.2.8.1.17.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.1.13.

10.1.2.2.3 End group call

10.1.2.2.3.1 Client originating procedures on-demand

When an MCPTT client wants to leave the MCPTT session that has been established using on-demand session, the MCPTT client shall follow the procedures as specified in subclause 6.2.4.1.

10.1.2.2.3.2 Client originating procedures using pre-established session

When an MCPTT client wants to leave the MCPTT session within a pre-established session, the MCPTT client shall follow the procedures as specified in subclause 6.2.4.2.

10.1.2.2.3.3 Client terminating procedures

Upon receiving a SIP BYE request for releasing the MCPTT chat session, the MCPTT client shall follow the procedures as specified in subclause 6.2.6.

10.1.2.3 Participating MCPTT function procedures

10.1.2.3.1 On-demand chat group call

10.1.2.3.1.1 MCPTT chat session establishment

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;

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" for a group identity identifying a chat MCPTT group containing an application/vnd.3gpp.mcptt-info+xml MIME body with the <session-type> element set to a value of "chat", 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 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 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 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 originating participating MCPTT function, the user identified by the MCPTT ID is not authorised to make chat 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 "108 user not authorised to make chat group calls" in a Warning header field as specified in subclause 4.4;

4) 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. 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 24.484 [50]) has been exceeded. If exceeded, the 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 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 for an exception to the limit for the maximum simultaneous MCPTT sessions supported for the MCPTT user.

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, 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 23.379 [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 document.

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 present in the incoming SIP INVITE request;

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

12) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request as specified in subclause 6.3.2.1.1.1;

13) if the received SIP INVITE request contains an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in Annex F.3; and

   a) if not already included, shall include a Content-Type header field set to "application/vnd.3gpp.location-info+xml"; and

   b) 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;

NOTE 8: Note that the application/vnd.3gpp.mcptt-info+xml MIME body will already have been copied into the outgoing SIP INVITE request by subclause 6.3.2.1.3.

14) 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 IETF RFC 4412 [29] set to the value indicated in the Resource-Priority header field of the SIP INVITE request from the MCPTT client; and

NOTE 9: The participating MCPTT function will leave verification of the Resource-Priority header field to the controlling MCPTT function.

15) 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 in step 14), 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 to the above SIP INVITE request in step 14) the participating MCPTT function:

1) if the 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 specified in the subclause 6.3.2.1.5.2 with the clarification that if an <MKFC-GKTPs> element was contained in the received SIP 200 (OK) response it is not included in the generated SIP 200 (OK) response;

NOTE 10: If an <MKFC-GKTPs> element is received, the participating MCPTT function essentially ignores it and does not forward it, resulting in unicast media plane transmission being used for the originating client.

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) 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;

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

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

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request in step 14) 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 the current procedure, shall perform the procedures of subclause 9.2.2.2.14.

10.1.2.3.1.2 Reception of a SIP re-INVITE request from served MCPTT client

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

Upon receipt of a SIP re-INVITE request for a served MCPTT client of a chat MCPTT group, 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 for terminating participating MCPTT function" 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 re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "true", the participating MCPTT function may by means beyond the scope of this specification choose to accept the request.

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. Otherwise, continue with the rest of the steps;

NOTE 2: If the received SIP re-INVITE request is received within a pre-established session associated with an MCPTT group session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

3) shall generate an outgoing SIP re-INVITE request as specified in subclause 6.3.2.1.9;

4) shall, if the SIP re-INVITE request was received within an on-demand session, include in the SIP re-INVITE request an SDP offer based on the SDP offer in the received SIP re-INVITE request as specified in subclause 6.3.2.1.1.1;

5) shall, if the SIP re-INVITE request was received within a pre-established session, include in the SIP re-INVITE request an SDP offer based upon the previously negotiated SDP for the pre-established session as specified in subclause 6.3.2.1.1.2;

6) if the received SIP re-INVITE request contains a Resource-Priority header field, shall include a Resource-Priority header field with the contents set as in the received Resource-Priority header field; and

NOTE 3: The controlling MCPTT function will determine the validity of the Resource-Priority header field.

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

Upon receipt of a SIP 2xx response to the above SIP re-INVITE request in step 7) the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as specified in the subclause 6.3.2.1.5.2;

2) if the SIP 200 (OK) response is to be sent within an on-demand session, shall include in the SIP 200 (OK) response an SDP answer as specified in the subclause 6.3.2.1.2.1;

3) if the SIP 200 (OK) response is to be sent within a pre-established session shall include in the SIP 200 (OK) response an SDP answer based upon the previously negotiated SDP for the pre-established session;

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

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

Upon receipt of a SIP 403 (Forbidden) response to the sent SIP re-INVITE request the participating MCPTT function:

1) shall generate a SIP 403 (Forbidden) response according to 3GPP TS 24.229 [4];

2) shall copy, if included in the received SIP 403 (Forbidden) response, the application/vnd.3gpp.mcptt-info+xml MIME body MIME body to the outgoing SIP (Forbidden) response;

3) shall include Warning header field(s) that were received in the incoming SIP 403 (Forbidden) response; and

4) shall forward the SIP 403 (Forbidden) response to the MCPTT client according to 3GPP TS 24.229 [4];

10.1.2.3.1.3 Reception of a SIP INVITE request for terminating MCPTT client

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

Upon receipt of a "SIP INVITE request for terminating participating MCPTT function", for a terminating MCPTT client of a chat MCPTT group, 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 for terminating participating MCPTT function" 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 application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "true", the participating MCPTT function can by means beyond the scope of this specification 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. Otherwise, continue with the rest of the steps;

3) 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;

NOTE 2: If an <MKFC-GKTPs> element is received, the participating MCPTT function essentially ignores it and does not forward it, resulting in unicast media plane transmission being used for the terminating client.

4) if:

   a) the invited MCPTT client has a pre-established session without an associated MCPTT session such that:

      i) the media-level section for the offered MCPTT speech media stream is the same as the media-level section for MCPTT speech media stream in the existing pre-established session; and

      ii) the media-level section of the offered media-floor control entity is the same as the media-level section for media-floor control entity in the existing pre-established session;

   then the participating MCPTT function may according to local policy perform the actions specified in subclause 10.1.2.3.2.2 and skip the remaining steps of the current procedure;

5) shall generate a SIP INVITE request as specified in subclause 6.3.2.2.3;

6) shall set the Request-URI to the public user identity associated with the MCPTT ID of the MCPTT user to be invited based on the contents of the Request-URI of the received "SIP INVITE request for terminating participating MCPTT function";

7) shall copy the contents of the P-Asserted-Identity header field of the incoming "SIP INVITE request for terminating participating MCPTT function" to the P-Asserted-Identity header field of the outgoing SIP INVITE request;

8) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received "SIP INVITE request for terminating participating MCPTT function" as specified in subclause 6.3.2.2.1;

9) if the received SIP INVITE request contains a Resource-Priority header field, shall include a Resource-Priority header field with the contents set as in the received Resource-Priority header field;

10) shall perform the procedures specified in subclause 6.3.2.2.9 to include any MIME bodies in the received SIP INVITE request; and

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

Upon receiving a SIP 200 (OK) response to the above SIP INVITE request sent to the MCPTT client, the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as described in the subclause 6.3.2.2.4.2;

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 6.3.2.2.2.1;

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

4) shall forward the SIP 200 (OK) response according to 3GPP TS 24.229 [4].

10.1.2.3.1.4 Reception of a SIP re-INVITE request for terminating MCPTT client

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

Upon receipt of a SIP re-INVITE request for a terminating MCPTT client of a chat MCPTT group, the participating MCPTT function:

1) shall check if a Resource-Priority header field is included in the incoming SIP re-INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

2) if the outgoing SIP re-INVITE request will be sent in the dialog of a pre-established session, perform the actions in subclause 10.1.2.3.2.2 and skip the remaining steps of the current procedure;

3) shall generate an outgoing SIP re-INVITE request as specified in subclause 6.3.2.2.10;

4) shall include in the SIP re-INVITE request an SDP offer based on the SDP offer in the received SIP re-INVITE request as specified in subclause 6.3.2.2.1; and

5) shall send the SIP re-INVITE request towards the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the above SIP re-INVITE request sent to the MCPTT client, the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as described in the subclause 6.3.2.2.4.2;

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 6.3.2.2.2.1; and

3) shall forward the SIP 200 (OK) response according to 3GPP TS 24.229 [4].

10.1.2.3.2 Chat group call within a pre-established session

10.1.2.3.2.1 MCPTT chat session establishment

Upon receipt of a "SIP REFER request for a pre-established session", with:

1) the Refer-To header containing a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [20] containing an <entry> element with a "uri" attribute containing a SIP-URI set to a chat group identity;

2) a body" URI header field of the SIP-URI specified above containing an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element set to "chat"; and

3) a Content-ID header field set to the "cid" URL;

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 REFER 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 1: If the application/vnd.3gpp.mcptt-info MIME body included in the SIP REFER request as described at the top of the present subclause contains an <emergency-ind> element or <imminentperil-ind> element 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 REFER request;

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 the participating MCPTT function cannot find a binding between the public user identity and an MCPTT ID or if the validity period of an existing binding has expired, then the participating MCPTT function shall reject the SIP REFER request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.4and shall not continue with any of the remaining steps;

4) if through local policy in the participating MCPTT function, the user identified by the MCPTT ID is not authorised to make chat group calls, shall reject the SIP REFER request with a SIP 403 (Forbidden) response to the SIP REFER request, with warning text set to "108 user not authorised to make group calls" in a Warning header field as specified in subclause 4.4.2;

5) shall retrieve the group identity within the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL contained in the Refer-To header field of the SIP REFER request;

6) 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 24.484 [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, and shall not continue with the rest of the steps;

7) if received SIP REFER request includes an application/vnd.3gpp.mcptt-info+xml MIME body with an <emergency-ind> element included or an <imminentperil-ind> element included, shall validate the request as described in subclause 6.3.2.1.8.3;

8) if the SIP REFER request contains in the application/vnd.3gpp.mcptt-info+xml MIME body:

   a) an <emergency-ind> element set to a value of "true" and this is an unauthorised request for an MCPTT emergency group call as determined by subclause 6.3.2.1.8.1;

   b) an <alert-ind> element set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as determined by subclause 6.3.2.1.8.2; or

   c) an <imminentperil-ind> element set to a value of "true" and this is an unauthorised request for an MCPTT imminent peril group call as determined by subclause 6.3.2.1.8.1;

   then shall reject the SIP REFER request with a SIP 403 (Forbidden) response and skip the rest of the steps;

9) if the user identified by the MCPTT ID is not affiliated to the group identified in the SIP REFER request as determined by subclause 9.2.2.2.11, shall perform the actions specified in subclause 9.2.2.2.12 for implicit affiliation;

10) if the actions for implicit affiliation specified in step 9) 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 REFER request 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 3: N2 is the total number of MCPTT groups that an MCPTT user can be affiliated to simultaneously as specified in 3GPP TS 23.379 [3].

NOTE 4: if the SIP REFER 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.

11) shall generate a final SIP 200 (OK) response to the "SIP REFER request for a pre-established session" according to 3GPP TS 24.229 [4];

12) if the "SIP REFER request for a pre-established session" contained a Refer-Sub header field containing the value "false" and a Supported header field containing "norefersub" value, shall handle the SIP REFER request as specified in 3GPP TS 24.229 [4], IETF RFC 3515 [25] as updated by IETF RFC 6665 [26], and IETF RFC 4488 [22] without establishing an implicit subscription;

13) shall determine the public service identity of the controlling MCPTT function associated with the group identity in the application/resource-lists MIME body pointed to by the "cid" URL in the Refer-To header field of the SIP REFER request. If the participating MCPTT function is unable to identify the controlling MCPTT function associated with the group identity, it shall reject the REFER request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.4, and shall not continue with the remaining steps;

NOTE 5: The public service identity can identify the controlling function in the primary MCPTT system or a partner MCPTT system.

NOTE 6: 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 document.

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

NOTE 7: In accordance with IETF RFC 4488 [22], the participating MCPTT function inserts the Refer-Sub header field containing the value "false" in the SIP 200 (OK) response to the SIP REFER request to indicate that it has not created an implicit subscription.

15) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.4;

16) shall set the Request-URI of the SIP INVITE request to the public service identity of the controlling MCPTT function associated with the group identity;

17) shall copy the group identity from the "uri" attribute of the <entry> element of the application/resource-lists MIME body pointed to by the "cid" URL in the Refer-to header field of the SIP REFER request, to the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body in the SIP INVITE request;

18) if the received SIP REFER request contained a Resource-Priority header field, 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 received SIP REFER request from the MCPTT client; and

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

Upon receipt of a SIP 2xx response to the above SIP INVITE request in step 19) the participating MCPTT function shall follow procedures specified in 3GPP TS 24.229 [4], with the clarifications given below:

1) shall cache the contact received in the Contact header field;

2) 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;

3) if the received SIP 2xx response was in response to a request for an MCPTT group call containing a Resource-Priority header field populated for an MCPTT emergency group call or MCPTT imminent peril group call as specified in subclause 6.3.2.1.8.4 and does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149":

   a) shall generate a SIP re-INVITE request to be sent towards the MCPTT client within the pre-established session as specified in subclause 6.3.2.1.8.5; and

   b) shall send the SIP re-INVITE request to the MCPTT client according to 3GPP TS 24.229 [4]; and

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

NOTE 8: There are two cases covered in the handling of the received SIP 2xx response above. The first case is when the SIP INVITE request sent to the controlling MCPTT function contained a Resource-Priority header field populated appropriately to request emergency level or imminent peril level priority but did not contain in the application/vnd.3gpp.mcptt-info+xml MIME body either an <emergency-ind> element or an <imminentperil-ind> element. The second case is when the SIP INVITE request sent to the controlling MCPTT function contained a Resource-Priority header field and contained either an <emergency-ind> element or an <imminentperil-ind> element. In either case, the received SIP 2xx response did not warn of a pending SIP INFO request.

Upon receipt of a SIP 302 (Moved Temporarily) response to the SIP INVITE request in step 19), the participating MCPTT function:

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

2) shall include in the SIP INVITE request an SDP offer based upon the SDP offer negotiated during the pre-established session establishment, any subsequent pre-established session modification and the SDP offer (if any) included in the"body" URI parameter of the SIP-URI contained in the <entry> element of the application/resource-lists MIME body, referenced by the "cid" URL in the Refer-To header field in the incoming SIP REFER request from the MCPTT client; and

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

Upon receiving a SIP INFO request from the controlling MCPTT function within the dialog of the SIP INVITE request for an MCPTT emergency call or MCPTT imminent peril call, the participating MCPTT function:

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

2) shall generate a SIP re-INVITE request to be sent towards the MCPTT client within the pre-established session as specified in subclause 6.3.2.1.8.5; and

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

NOTE 9: This is the case where the SIP REFER request previously received from the MCPTT client contained a Resource-Priority header field populated for an MCPTT emergency group call or MCPTT imminent peril group call as specified in subclause 6.3.2.1.8.4 but was also a request for either an MCPTT emergency group call or an MCPTT imminent peril group call.

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

1) if the implicit affiliation procedures of subclause 9.2.2.2.12 were invoked in the present subclause, shall perform the procedures of subclause 9.2.2.2.14; and

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

10.1.2.3.2.2 MCPTT chat session establishment for terminating user within a pre-established session

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

1) 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.

NOTE 1: If an <MKFC-GKTPs> element is received, the participating MCPTT function essentially ignores it and does not forward it, resulting in unicast media plane transmission being used for the terminating client.

Upon receipt of a SIP INVITE request or a SIP re-INVITE request for a terminating MCPTT client of a chat MCPTT group using a pre-established session, the participating MCPTT function:

1) shall generate an outgoing SIP re-INVITE request as specified in subclause 6.3.2.2.10 to be sent within the dialog of the pre-established session;

2) if the received SIP INVITE request or SIP re-INVITE request contains a Resource-Priority header field, shall include a Resource-Priority header field with the contents set as in the received Resource-Priority header field;

3) shall include in the SIP re-INVITE request an SDP offer based on the SDP offer in the received SIP INVITE request or SIP re-INVITE request as specified in subclause 6.3.2.1.1.2; and

NOTE 2: The media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as in the existing pre-established session as per the conditions for pre-established session usage specified in subclause 10.1.2.3.1.3.

4) shall send the SIP re-INVITE request towards the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the above SIP re-INVITE request sent to the MCPTT client, the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as described in the subclause 6.3.2.2.4.2;

2) shall include in the SIP 200 (OK) response an SDP answer as specified in subclause 6.3.2.2.2.2; and

3) shall send the SIP 200 (OK) response according to 3GPP TS 24.229 [4].

10.1.2.3.3 End group call at the originating participating MCPTT function

10.1.2.3.3.1 Receipt of SIP BYE request for ending on-demand chat session

Upon receiving from the MCPTT client a SIP BYE request the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.1.6.

10.1.2.3.3.2 Receipt of SIP REFER "BYE" request for ending chat session using pre-established session

Upon receiving from the MCPTT client a SIP REFER request when using a pre-established session with the method SIP-URI parameter set to value "BYE" in the URI in the Refer-To header field the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.1.7.

10.1.2.3.4 End group call at the terminating participating MCPTT function

10.1.2.3.4.1 Receipt of SIP BYE request for on-demand chat session

Upon receiving a SIP BYE request from the controlling MCPTT function, the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.2.8.1.

10.1.2.3.4.2 Receipt of SIP BYE request for ongoing pre-established session

Upon receiving a SIP BYE request from the controlling MCPTT function and if the MCPTT session id refers to an MCPTT user that has a pre-established session with the participating MCPTT function, the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.2.8.2.

10.1.2.4 Controlling MCPTT function procedures

10.1.2.4.1 On-demand chat group call

10.1.2.4.1.1 Procedure for establishing an MCPTT chat session and procedure for joining an established MCPTT chat session

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) 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

5) alert indication in an incoming SIP INVITE request refers to the <alert-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" containing a group identity identifying a chat MCPTT group, the controlling 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 controlling 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 skip the rest of the steps;

NOTE 1: If the SIP INVITE request contains an emergency indication set to a value of "true", the controlling MCPTT function can by means beyond the scope of this specification choose to accept the request.

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag;

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt"; or

   c) the isfocus media feature tag is present in the Contact header field;

3) if received SIP INVITE request includes an application/vnd.3gpp.mcpttinfo+xml MIME body with an <emergency-ind> element included or an <imminentperil-ind> element included, shall validate the request as described in subclause 6.3.3.1.17;

4) 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 and continue with the rest of the steps if the checks in subclause 6.3.5.2 succeed;

5) if the MCPTT user identified by the MCPTT ID in the SIP INVITE request is not affiliated with the MCPTT group identified by the group identity in the SIP INVITE request as determined by the procedures of subclause 6.3.6:

   a) shall check if the MCPTT user is eligible to be implicitly affiliated with the MCPTT chat group as determined by subclause 9.2.2.3.6; and

   b) if the MCPTT user is not eligible for implicit affiliation, shall reject the SIP INVITE request with 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;

6) if the SIP INVITE request contains unauthorised request for an MCPTT emergency group call as determined by subclause 6.3.3.1.13.2:

   a) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response as specified in subclause 6.3.3.1.14; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

7) if the SIP INVITE request contains an unauthorised request for an MCPTT imminent peril group call as determined by subclause 6.3.3.1.13.6, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response with the following clarifications:

   a) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "false"; and

b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

8) if a Resource-Priority header field is included in the SIP INVITE request:

a) if the Resource-Priority header field is set to the value indicated for emergency calls and the SIP INVITE request does not contain an emergency indication and the in-progress emergency state of the group is set to a value of "false", shall reject the SIP INVITE request with a SIP 403 (Forbidden) response and skip the remaining steps; and

b) if the Resource-Priority header field is set to the value indicated for imminent peril calls and the SIP INVITE request does not contain an imminent peril indication and the in-progress imminent peril state of the group is set to a value of "false", shall reject the SIP INVITE request with a SIP 403 (Forbidden) response; and skip the remaining steps;

9) 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;

10) shall create a chat group session and allocate an MCPTT session identity for the chat group session if the MCPTT chat group session identity does not already exist, and may handle timer TNG3 (group call timer) as specified in subclause 6.3.3.5;

11) if the chat group session is ongoing and the <on-network-max-participant-count> as specified in 3GPP TS 24.481 [31] is already reached:

a) if, according to local policy, the user identified by the MCPTT ID in the SIP INVITE request is deemed to have a higher priority than an existing user in the chat group session, may remove a participant from the session by following subclause 10.1.1.4.4.3, and skip the next step; and

NOTE 2: The local policy for deciding whether to admit a user to a call that has reached its maximum amount of participants can include the <user-priority> and the <participant-type> of the user as well as other information of the user from the group document as specified in 3GPP TS 24.481 [31]. The local policy decisions can also include taking into account whether the imminent-peril indicator or emergency indicator was received in the SIP INVITE request.

b) shall return a SIP 486 (Busy Here) response with the warning text set to "122 too many participants" to the originating network as specified in subclause 4.4 Otherwise, continue with the rest of the steps;

12) if the received SIP INVITE request was determined to be eligible for implicit affiliation in step 5) and if subclause 9.2.2.3.7 was not previously invoked in the present subclause, shall perform the implicit affiliation as specified in subclause 9.2.2.3.7;

13) if the SIP INVITE request contains an emergency indication set to a value of "true" or the in-progress emergency state of the group to "true" the controlling MCPTT function shall:

a) validate that the SIP INVITE request includes a Resource-Priority header field populated with the values for an MCPTT emergency group call as specified in subclause 6.3.3.1.19, and if not:

i) perform the actions specified in subclause 6.3.3.1.8;

ii) send the SIP UPDATE request generated in subclause 6.3.3.1.8 towards the initiator of the SIP INVITE request according to 3GPP TS 24.229 [4]; and

iii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in subclause 6.3.3.1.8, proceed with the rest of the steps.

NOTE 3: Verify that the Resource-Priority header is included and properly populated for both ongoing and newly-entered in-progress emergency states of the specified group.

b) if the in-progress emergency state of the group is set to a value of "true" and the MCPTT user is indicating a new emergency indication:

i) for each of the other affiliated members of the group generate a SIP MESSAGE request notification of the MCPTT user's emergency indication as specified in subclause 6.3.3.1.11 with the following clarifications:

A) set the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "true";

B) if the received SIP INVITE contains an alert indication set to a value of "true" and this is an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, perform the procedures specified in subclause 6.3.3.1.12; and

C) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4];

ii) cache the information that the MCPTT user has initiated an MCPTT emergency call; and

iii) if the SIP INVITE request contains an authorised request for an MCPTT emergency alert as determined in step i) B) above, cache the information that the MCPTT user has initiated an MCPTT emergency alert; and

c) if the in-progress emergency state of the group is set to a value of "false":

i) shall set the value of the in-progress emergency state of the group to "true";

ii) shall start timer TNG2 (in-progress emergency group call timer) and handle its expiry as specified in subclause 6.3.3.1.16;

iii) shall generate SIP re-INVITE requests for the MCPTT emergency group call to the other affiliated and joined participants of the chat MCPTT group as specified in subclause 6.3.3.1.6;

iv) shall generate SIP INVITE requests for the MCPTT emergency group call to the affiliated but not joined members of the chat MCPTT group as specified in subclause 6.3.3.1.7;

A) for each affiliated but not joined member shall send the SIP INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

B) upon receiving a SIP 200 (OK) response to the SIP INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5];

v) shall cache the information that the MCPTT user has initiated an MCPTT emergency call; and

vi) if the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body is set to "true" and is an authorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall cache the information that the MCPTT user has initiated an MCPTT emergency alert; and

vii) if the in-progress imminent peril state of the group is set to a value of "true", shall set it to a value of "false";

14) if the in-progress emergency state of the group is set to a value of "false" and if the SIP INVITE request contains an imminent peril indication set to a value of "true" or the in-progress imminent peril state of the group is set to "true", the controlling MCPTT function shall:

a) validate that the SIP INVITE request includes 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 if not:

i) perform the actions specified in subclause 6.3.3.1.8;

ii) send the SIP UPDATE request generated in subclause 6.3.3.1.8 towards the initiator of the SIP INVITE request according to 3GPP TS 24.229 [4]; and

iii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in subclause 6.3.3.1.8 proceed with the rest of the steps.

NOTE 4: Verify that the Resource-Priority header is included and properly populated for both ongoing and newly-entered in-progress imminent peril states of the specified group.

b) if the in-progress imminent peril state of the group is set to a value of "true" and the MCPTT user is indicating a new imminent peril indication:

i) for each of the other affiliated member of the group generate a SIP MESSAGE request notification of the MCPTT user's imminent peril indication as specified in subclause 6.3.3.1.11 with the following clarifications;

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

B) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4]; and

ii) cache the information that the MCPTT user has initiated an MCPTT imminent peril call; and

c) if the in-progress imminent peril state of the group is set to a value of "false":

i) shall set the value of the in-progress imminent peril state of the group to "true";

ii) shall generate SIP re-INVITE requests for the MCPTT imminent peril group call to the other affiliated and joined participants of the chat MCPTT group as specified in subclause 6.3.3.1.15;

iii) shall generate SIP INVITE requests for the MCPTT imminent peril call to the affiliated but not joined members of the chat MCPTT group as specified in subclause 6.3.3.1.7;

A) for each affiliated but not joined member shall send the SIP INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

B) Upon receiving a SIP 200 (OK) response to the SIP INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

iv) shall cache the information that the MCPTT user has initiated an MCPTT imminent peril call;

15) shall accept the SIP request and generate a SIP 200 (OK) response to the SIP INVITE request according to 3GPP TS 24.229 [4];

16) shall include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.3.3.2.1 unless the procedures of subclause 6.3.3.1.8 were performed in step 13)a) or step 14)a) above;

17) should include the Session-Expires header field and start supervising the SIP session 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";

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

19) shall include the following in a 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";

c) the MCPTT session identity; and

d) the media feature tag isfocus;

20) shall include the "tdialog" option tag in a Supported header field according to IETF RFC 4538 [23];

21) if the SIP INVITE request contains an alert indication set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

22) if the received SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "true" and if the in-progress emergency state of the group is set to a value of "true", shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

NOTE 5: In this case, the request was for an imminent peril call but a higher priority MCPTT emergency call was already in progress on the group. Hence, the imminent peril call request aspect of the request is denied but the request is granted with emergency level priority.

23) shall interact with media plane as specified in 3GPP TS 24.380 [5];

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

25) if the chat group session was already ongoing and if at least one of the participants has subscribed to the conference event package, shall send a SIP NOTIFY request to all participants with a subscription to the conference event package as specified in subclause 10.1.3.4.2.

Upon receiving a SIP ACK to the SIP 200 (OK) response sent towards the inviting MCPTT client, and the SIP 200 (OK) response was sent with the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.18.

10.1.2.4.1.2 Receipt of a SIP re-INVITE request

In the procedures in this subclause:

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

Upon receipt of a SIP re-INVITE request for an MCPTT session identity identifying a chat MCPTT group session, the controlling 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 re-INVITE request with a SIP 500 (Server Internal Error) response. The controlling 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 skip the rest of the steps;

NOTE 1: if the SIP re-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 an MCPTT emergency group call as determined by subclause 6.3.3.1.13.2, or for originating an MCPTT imminent peril group call as determined by subclause 6.3.3.1.13.5, the controlling MCPTT function can according to local policy choose to accept the request.

2) if the received SIP re-INVITE request includes an application/vnd.3gpp.mcptt-info+xml MIME body with an <emergency-ind> element included or an <imminentperil-ind> element included, shall validate the request as described in subclause 6.3.3.1.17;

3) if the SIP re-INVITE request contains an unauthorised request for an MCPTT emergency call as determined by subclause 6.3.3.1.13.2:

   a) shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response as specified in subclause 6.3.3.1.14; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

4) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "true" and is an authorised request to initiate an MCPTT emergency group call as determined by subclause 6.3.3.1.13.2, the controlling MCPTT function shall:

   a) validate that the SIP re-INVITE request includes a Resource-Priority header field is populated correctly for an MCPTT emergency group call as specified in subclause 6.3.3.1.19, and if not:

      i) shall perform the actions specified in subclause 6.3.3.1.8; and

      ii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in subclause 6.3.3.1.8 shall proceed with the rest of the steps.

NOTE 2: Verify that the Resource-Priority header is included and properly populated for both ongoing and newly-entered in-progress emergency states of the specified group.

   b) if the in-progress emergency state of the group is set to a value of "true" and the MCPTT user is indicating a new emergency indication:

      i) shall cache the MCPTT ID of the MCPTT user that has initiated an MCPTT emergency call;

ii) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "true" and is an authorised request for an MCPTT emergency alert as determined by subclause 6.3.3.1.13.1, shall cache the MCPTT ID of the MCPTT user that has initiated an MCPTT emergency alert; and

iii) for each of the other affiliated members of the group, generate a SIP MESSAGE request notification of the MCPTT user's emergency indication as specified in subclause 6.3.3.1.11 with the following clarifications:

A) set the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "true";

B) if the received SIP re-INVITE contains an alert indication set to a value of "true" and this is an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, perform the procedures specified in subclause 6.3.3.1.12; and

C) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4]; and

c) if the in-progress emergency state of the group is set to a value of "false":

i) shall set the value of the in-progress emergency state of the group to "true";

ii) shall cache the MCPTT ID of the MCPTT user that has initiated an MCPTT emergency call;

iii) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "true" and this is an authorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall cache the MCPTT ID of the MCPTT user that has initiated an MCPTT emergency alert;

iv) shall start timer TNG2 (in-progress emergency group call timer) and handle its expiry as specified in subclause 6.3.3.1.16;

v) shall generate SIP re-INVITE requests for the MCPTT emergency group call to the other affiliated and joined participants of the chat MCPTT group as specified in subclause 6.3.3.1.6. The MCPTT controlling function:

A) for each affiliated and joined member shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

B) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

vi) shall generate SIP INVITE requests for the MCPTT emergency group call to the affiliated but not joined members of the chat MCPTT group as specified in subclause 6.3.3.1.7. The controlling MCPTT function:

A) for each affiliated but not joined member shall send the SIP INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

B) Upon receiving a SIP 200 (OK) response to the SIP INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

vii)if the in-progress imminent peril state of the group is set to a value of "true", shall set it to a value of "false";

5) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "false" and is an unauthorised request for an MCPTT emergency group call cancellation as determined by subclause 6.3.3.1.13.4:

a) shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response;

b) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in annex F.1 with an <emergency-ind> element set to a value of "true";

c) if an <alert-ind> element of the mcpttinfo MIME body is included set to "false" and there is an outstanding MCPTT emergency alert for the MCPTT user, shall include in the application/vnd.3gpp.mcptt-info+xml MIME body and <alert-ind> element set to a value of "true"; and

d) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

6) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "false" and is determined to be an authorised request for an MCPTT emergency call cancellation as specified in subclause 6.3.3.1.13.4 and the in-progress emergency state of the group to is set to a value of "true" the controlling MCPTT function shall:

a) validate that the SIP re-INVITE request includes a Resource-Priority header field is populated correctly for a normal priority MCPTT group call as specified in subclause 6.3.3.1.19, and if not:

i) shall perform the actions specified in subclause 6.3.3.1.8; and

ii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in subclause 6.3.3.1.8 shall proceed with the rest of the steps;

NOTE 3: Verify that the Resource-Priority header is included and properly populated for an in-progress emergency state cancellation of the specified group.

b) shall set the in-progress emergency group state of the group to a value of "false";

c) shall clear the cache of the MCPTT ID of the MCPTT user identified by the <originated-by> element as having an outstanding MCPTT emergency group call;

d) if an <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body is included and set to "false" and is determined to be an authorised request for an MCPTT emergency alert cancellation as specified in subclause 6.3.3.1.13.3 and there is an outstanding MCPTT emergency alert for the MCPTT user shall:

i) if the received SIP re-INVITE request contains an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, clear the cache of the MCPTT ID of the MCPTT user identified by the <originated-by> element as having an outstanding MCPTT emergency alert; and

ii) if the received SIP re-INVITE request does not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, clear the cache of the MCPTT ID of the sender of the SIP re-INVITE request as having an outstanding MCPTT emergency alert;

e) shall generate SIP re-INVITE requests to the other affiliated and joined members of the MCPTT group as specified in subclause 6.3.3.1.6. The MCPTT controlling function:

i) for each affiliated and joined member shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

NOTE 4: Subclause 6.3.3.1.6 will inform the affiliated and joined members of the cancellation of the MCPTT group's in-progress emergency state and the cancellation of the MCPTT emergency alert if applicable.

f) for each of the affiliated but not joined members of the group shall:

i) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's emergency call as specified in subclause 6.3.3.1.11;

ii) set the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false";

iii) if indicated above in step d), set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false"; and

iv) send the SIP MESSAGE request according to 3GPP TS 24.229 [4];

7) if a Resource-Priority header field is included in the SIP re-INVITE request:

a) if the Resource-Priority header field is set to the value indicated for emergency calls and the received SIP re-INVITE request does not contain an authorised request for an MCPTT emergency call as determined in step 4) above and the in-progress emergency state of the group is set to a value of "false", shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response and skip the remaining steps; or

b) if the Resource-Priority header field is set to the value indicated for imminent peril calls and the received SIP re-INVITE request does not contain an authorised request for an MCPTT imminent peril call as determined by the procedures of subclause 6.3.3.1.13.5 and the in-progress imminent peril state of the group is set to a value of "false", shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response and skip the remaining steps;

8) if the received SIP re-INVITE request contains an imminent peril indication, shall perform the procedures specified in subclause 10.1.2.4.1.3 and skip the rest of the steps;

9) shall include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.3.3.2.1 unless the procedures of subclause 6.3.3.1.8 were performed in step 6) a) i) above;

10) shall include the "tdialog" option tag in a Supported header field according to IETF RFC 4538 [23];

11) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "true" and if this is an unauthorised request for an MCPTT emergency alert as determined by subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

12) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "false" and if this is an unauthorised request for an MCPTT emergency alert cancellation as determined by subclause 6.3.3.1.13.3, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

13) if the received SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "true", this is an authorised request for an MCPTT imminent peril group call and if the in-progress emergency state of the group is set to a value of "true", shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

NOTE 5: In this case, the request was for an imminent peril call but a higher priority MCPTT emergency call was already in progress on the group. Hence, the imminent peril call request aspect of the request is denied but the request is granted with emergency level priority.

14) shall interact with media plane as specified in 3GPP TS 24.380 [5]; and

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

Upon receiving a SIP ACK to the SIP 200 (OK) response sent towards the inviting MCPTT client, and the SIP 200 (OK) response was sent with the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.18.

10.1.2.4.1.3 Handling of a SIP re-INVITE request for imminent peril session

In the procedures in this subclause:

1) 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.

When the controlling function receives a SIP re-INVITE request with and imminent peril indication, the controlling function:

1) if the SIP re-INVITE request contains an unauthorised request for an MCPTT imminent peril group call as determined by subclause 6.3.3.1.13.5, shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response with the following clarifications:

   a) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in Annex F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "false"; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

2) if the in-progress emergency group state of the group is set to a value of "false" and if the SIP re-INVITE request contains an imminent peril indication set to a value of "true" or the in-progress imminent peril state of the group to "true", the controlling MCPTT function shall:

   a) validate that the SIP re-INVITE request includes a Resource-Priority header field with the namespace set to the MCPTT-specific namespace specified in IETF RFC 8101 [48] and the priority set to the priority designated for imminent peril calls and if not:

      i) perform the actions specified in subclause 6.3.3.1.8;

      ii) send the SIP UPDATE request generated in subclause 6.3.3.1.8 towards the initiator of the SIP re-INVITE request according to 3GPP TS 24.229 [4]; and

      iii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in subclause 6.3.3.1.8 proceed with the rest of the steps.

NOTE 3: Verify that the Resource-Priority header is included and properly populated for both ongoing and newly-entered in-progress imminent peril states of the specified group.

   b) if the in-progress imminent peril state of the group is set to a value of "true" and the MCPTT user is indicating a new imminent peril indication:

      i) for each of the other affiliated member of the group generate a SIP MESSAGE request notification of the MCPTT user's imminent peril indication as specified in subclause 6.3.3.1.11 with the following clarifications;

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

         B) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4]; and

      ii) cache the information that the MCPTT user has initiated an MCPTT imminent peril call; and

   c) if the in-progress imminent peril state of the group is set to a value of "false":

      i) shall set the value of the in-progress imminent peril state of the group to "true";

      ii) shall generate SIP re-INVITE requests for the MCPTT imminent peril group call to the other affiliated and joined participants of the chat MCPTT group as specified in subclause 6.3.3.1.15;

      iii) shall generate SIP INVITE requests for the MCPTT imminent peril group call to the affiliated but not joined members of the chat MCPTT group as specified in subclause 6.3.3.1.7;

         A) for each affiliated but not joined member shall send the SIP INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

         B) Upon receiving a SIP 200 (OK) response to the SIP INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

      iv) shall cache the information that the MCPTT user has initiated an MCPTT imminent peril call;

3) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "false" and is an unauthorised request for an MCPTT imminent peril group call cancellation as determined by subclause 6.3.3.1.13.6 shall:

   a) reject the SIP re-INVITE request with a SIP 403 (Forbidden) response to the SIP re-INVITE request; and

   b) include in the SIP 403 (Forbidden) response:

      i) include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in Annex F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <imminentperil-ind> element set to a value of "false";

      ii) send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4]; and

      iii) skip the rest of the steps;

4) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "false" and is determined to be an authorised request for an MCPTT imminent peril call cancellation as specified in subclause 6.3.3.1.13.6 and the in-progress imminent peril state of the group to is set to a value of "true" the controlling MCPTT function shall:

   a) validate that the SIP re-INVITE request includes a Resource-Priority header field with the namespace set to the MCPTT-specific namespace specified in IETF RFC 8101 [48], and the priority set to the priority level designated for a normal priority MCPTT group call, and if not:

      i) shall perform the actions specified in subclause 6.3.3.1.8; and

      ii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in subclause 6.3.3.1.8 shall proceed with the rest of the steps;

NOTE 3: verify that the Resource-Priority header is included and properly populated for an in-progress emergency group state cancellation of the specified group.

   b) shall set the in-progress imminent peril state of the group to a value of "false";

   c) shall cache the information that the MCPTT user no longer has an outstanding MCPTT imminent peril group call;

   d) shall generate SIP re-INVITES requests to the other affiliated and joined members of the MCPTT group as specified in subclause 6.3.3.1.15. The MCPTT controlling function:

      i) for each affiliated and joined member shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

      ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

NOTE 4: subclause 6.3.3.1.15 will inform the affiliated and joined members of the cancellation of the MCPTT group's in-progress emergency group state and the cancellation of the MCPTT emergency alert if applicable.

   e) for each of the affiliated but not joined members of the group shall:

      i) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's imminent peril call as specified in subclause 6.3.3.1.11;

      ii) set the <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false"; and

      iii) send the SIP MESSAGE request according to 3GPP TS 24.229 [4];

5) shall include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [4] with the clarifications specified in subclause 6.3.3.2.1 unless the procedures of subclause 6.3.3.1.8 were performed in step 2) or 4) above;

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

7) shall include the "tdialog" option tag in a Supported header field according to IETF RFC 4538 [23];

8) shall interact with media plane as specified in 3GPP TS 24.380 [5]; and

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

10.1.2.4.2 End group call at the terminating controlling MCPTT function

Upon receiving a SIP BYE request the controlling MCPTT function shall follow the procedures as specified in subclause 6.3.3.2.4.

10.1.2.4.3 End group call initiated by the controlling MCPTT function

10.1.2.4.3.1 General

This subclause describes the procedures of each functional entity for ending the group call initiated by the controlling MCPTT function.

10.1.2.4.3.2 SIP BYE request for releasing MCPTT session for a group call

When the MCPTT session for group call needs to be released as specified in subclause 6.3.8.1, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.5.

10.1.2.4.3.3 SIP BYE request toward a MCPTT client

When an MCPTT client needs to be removed from the MCPTT session (e.g. due to de-affiliation or admitting a higher priority user), the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.5.

After successful removing the MCPTT client from the MCPTT session, the controlling MCPTT function may generate a notification to the MCPTT clients, which have subscribed to the conference state event package that an MCPTT user has been removed from the MCPTT session, as specified in subclause 6.3.3.4 and send the SIP NOTIFY request to the MCPTT client according to 3GPP TS 24.229 [4].

10.1.2.5 Non-controlling function of an MCPTT group procedures

10.1.2.5.1 Terminating procedures

10.1.2.5.1.1 General

When receiving the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" the MCPTT server can be acting as a controller MCPTT function in an ongoing chat group call or, if a chat group call is not ongoing, be initiated as an non-controlling MCPTT function and invite MCPTT users.

If a chat group call is not ongoing the MCPTT server shall perform the actions specified in subclause 10.1.2.5.1.2.

If the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" is received when a chat group call is ongoing, the controlling MCPTT function may switch from operating in a controlling MCPTT function mode to operate in a non-controlling MCPTT function mode as specified in subclause 10.1.2.5.1.3.

When operating in the non-controlling mode and a SIP BYE request is received from the controlling MCPTT function, the non-controlling MCPTT function shall change from operating in the non-controlling mode to operating in the controlling mode as specified in subclause 10.1.2.5.1.4.

10.1.2.5.1.2 Initiating a chat group session

Upon receipt of a "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" and if a chat group call is not ongoing, the non-controlling MCPTT function of an MCPTT group:

NOTE 1: The Contact header field of the SIP INVITE request contains the "isfocus" feature media tag.

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 controlling 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;

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. Otherwise, continue with the rest of the steps;

3) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag; or

b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

4) if the partner MCPTT system does not have a mutual aid relationship with the primary MCPTT system identified by the contents of the P-Asserted-Identity, shall reject the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" with a SIP 403 (Forbidden) response, with warning text set to "128 isfocus already assigned" in a Warning header field as specified in subclause 4.4, and shall not process the remaining steps;

5) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

6) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.4.2.2.2 before continuing with the rest of the steps;

7) 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 6.3.4.2.1;

8) shall interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3.5; and

NOTE 2: Resulting media plane processing is completed before the next step is performed.

9) shall send a SIP 200 (OK) response to the controlling MCPTT function according to 3GPP TS 24.229 [4].

10.1.2.5.1.3 Joining an ongoing chat group call

Upon receipt of a "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" and if a chat group call is already ongoing, the non-controlling MCPTT function of an MCPTT group:

NOTE 1: The Contact header field of the SIP INVITE request contains the "isfocus" feature media tag.

1) 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. Otherwise, continue with the rest of the steps;

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

3) if the partner MCPTT system does not have a mutual aid relationship with the primary MCPTT system identified by the contents of the P-Asserted-Identity, shall reject the "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" with a SIP 403 (Forbidden) response, with warning text set to "128 isfocus already assigned" in a Warning header field as specified in subclause 4.4, and shall not process the remaining steps;

4) shall cache the content of the SIP INVITE request, if received in the Contact header field and if the specific feature tags are supported;

5) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

6) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.4.2.2.2 before continuing with the rest of the steps;

7) 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 6.3.4.2.1;

8) shall instruct the media plane to initialise the switch to the non-controlling mode as specified in 3GPP TS 24.380 [5] subclause 6.5.2.3;

NOTE 2: Resulting media plane processing is completed before the next step is performed. The media plane indicates the state of the floor and if the state is "floor-taken", information about the current speaker(s).

9) if the media plane provided information about the current speaker(s), cache the information about the current speaker(s); and

10) shall send a SIP 200 (OK) response to the controlling MCPTT function according to 3GPP TS 24.229 [4].

Upon receipt of the SIP ACK request, the non-controlling MCPTT function of an MCPTT group:

1) if information about a current speaker(s) is cached:

   a) shall generate a SIP INFO request as specified in subclause 6.3.4.1.3; and

   b) shall send the SIP INFO request to the controlling MCPTT function as specified in 3GPP TS 24.229 [4];

2) shall instruct the media plane to finalise the switch to the non-controlling mode as specified in 3GPP TS 24.380 [5] subclause 6.3.5.3; and

3) if at least one of the MCPTT clients in the chat group session has a subscription to the conference event package, shall subscribe to the conference event package from the controlling MCPTT function as specified in subclause 10.1.3.5.3.

10.1.2.5.1.4 Splitting an ongoing chat group call

Upon receipt of a SIP BYE request, the non-controlling MCPTT function of an MCPTT group:

1) if keeping the chat group call active is according to the release policy in subclause 6.3.8.1, shall request media plane to switch to controlling mode as specified in 3GPP TS 24.380 [5] subclause 6.3.5;

NOTE 1: Resulting media plane processing is completed before the next step is performed.

2) shall send a SIP 200 (OK) response to the SIP BYE request; and

3) if at least one MCPTT client has subscribed to the conference package, shall send a NOTIFY request to all participants with a subscription to the conference event package as specified in subclause 10.1.3.5.2.

NOTE 2: The SIP NOTIFY request will indicate that all participants, with the exception of the MCPTT users belonging to the constituent MCPTT group hosted by the non-controlling MCPTT function, have left the group session.

10.1.2.5.1.5 MCPTT client joining the temporary group chat session

When acting in the non-controlling connection mode when receiving of a "SIP INVITE request for controlling MCPTT function of an MCPTT group" containing a group identity identifying a constituent chat MCPTT group being part of the temporary group call, the non-controlling MCPTT function shall act as a controlling MCPTT function towards the MCPTT client and shall perform the actions in the subclause 10.1.2.4.1.1 with the following clarifications:

1) the MCPTT session identity in the Contact header field of the SIP 200 (OK) response shall be the MCPTT session identity generated by the non-controlling MCPTT function; and

2) the subclause 10.1.3.5.2 shall be used when sending the SIP NOTIFY request for subscriptions to the conference event package.

10.1.2.5.1.6 Receipt of a SIP re-INVITE request from an MCPTT client

Upon receipt of a SIP re-INVITE request from an MCPTT client the non-controlling MCPTT function shall act as the controlling MCPTT function and shall perform the actions in subclause 10.1.2.4.1.2.

10.1.2.5.1.7 SIP OPTIONS request authorization procedure

Upon receipt of an SIP OPTIONS request containing a P-Asserted-Identity header field containing the public service identity of a MCPTT server authorized to send the OPTIONS request, the non-controlling MCPTT function shall perform the actions in subclause 10.1.1.5.4 otherwise the non-controlling MCPTT function shall send a SIP 403 (Forbidden) response as specified in 3GPP TS 24.229.

10.1.2.5.1.8 Initiating a temporary group session

Upon receiving a "SIP INVITE request for controlling MCPTT function of an MCPTT group" when a chat group session is not ongoing, the non-controlling MCPTT-function shall:

NOTE 1: The difference between a "SIP INVITE request for controlling MCPTT function of an MCPTT group" and a "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" is that the latter SIP INVITE request contains the isfocus media feature tag in the Contact header field.

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 non-controlling 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;

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. Otherwise, continue with the rest of the steps;

3) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if:

   a) an Accept-Contact header field does not include the g.3gpp.mcptt media feature tag; or

   b) an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

4) shall retrieve the group document from the group management server for the MCPTT group ID contained in the <mcptt-request-uri> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request and carry out initial processing as specified in subclause 6.3.5.2 and continue with the rest of the steps if the checks in subclause 6.3.5.2 succeed;

NOTE 2: If the checks are not succesful, the SIP response to the "SIP INVITE request for controlling MCPTT function of an MCPTT group" is already sent in the subclause 6.3.5.2.

5) shall cache the content of the SIP INVITE request;

6) shall check if a Resource-Priority header field is included in the incoming SIP INVITE request and may apply any preferential treatment to the SIP request as specified in 3GPP TS 24.229 [4];

7) shall authorize the MCPTT user in the <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the "SIP INVITE request for controlling MCPTT function of an MCPTT group" as specified in subclause 6.3.5.2, if the MCPTT user is unauthorized to join a chat group session, the non-controlling MCPTT function shall send a SIP 403 (Forbidden) response with the warning text set to "106 user not authorised to join chat group" in a Warning header field as specified in subclause 4.4.

8) shall generate a SIP INVITE request to the controlling MCPTT function as specified in subclause 6.3.4.1.4; and

9) shall send the SIP INVITE request to the controlling MCPTT function as specified in 3GPP TS 24.229 [4].

Upon receipt of a SIP 2xx response to the SIP INVITE request sent to the controlling MCPTT function as specified above, the non-controlling MCPTT function:

1) shall send the SIP ACK request to the controlling MCPTT function as specified in 3GPP TS 24.229 [4];

2) shall generate a SIP 200 (OK) to the "SIP INVITE request for controlling MCPTT function of an MCPTT group" as specified in 3GPP TS 24.229 populated as follows:

   a) shall include an SDP answer as specified in subclause 6.3.4.2.1 based on the SDP answer in the SIP 200 (OK) response;

   b) shall include the public service identifier of the non-controlling MCPTT function in the P-Asserted-Identity header field; and

   c) shall include the warning text set to "148 MCPTT group is regrouped" in a Warning header field as specified in subclause 4.4; and

NOTE 3: As long as the MCPTT group is regrouped the floor control messages in the media plane includes a grouped regrouped indication as specified in 3GPP TS 24.380 [5].

3) shall start acting as a non-controlling MCPTT function and interact with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.5.

Upon receipt of other final SIP responses with the exception of the SIP 2xx response to the INVITE request sent to the controlling MCPTT function as specified above, the non-controlling MCPTT function:

1) shall send the SIP ACK response to the controlling MCPTT function as specified in 3GPP TS 24.229 [4]; and

2) perform the actions in the subclause 10.1.1.5.2.4.

NOTE 4: Regardless if the controlling MCPTT function accepts or rejects the SIP INVITE request sent above the prearranged group session continues to be initiated with only the members of the group homed on the non-controlling MCPTT function of the group being invited to the group call.

10.1.3 Subscription to the conference event package

10.1.3.1 General

The IETF RFC 4575 [30] defines a conference state event package that shall be used to obtain the status of participants in group sessions.

The MCPTT client may subscribe to the conference state event package at any time in a group session that the MCPTT client participates in. The subclause 10.1.3.2 specifies the procedures in the MCPTT client when subscribing to the conference events.

The participating MCPTT function shall forward conference state subscriptions and notifications as specified in subclause 10.1.3.3.

The controlling MCPTT function shall handle subscriptions and notification of conference state events as specified in subclause 10.1.3.4.

The non-controlling MCPTT function shall handle subscriptions and notification of conference state events as specified in subclause 10.1.3.5.

When the non-controlling MCPTT function connection model is used, the controlling MCPTT function subscribes to the conference state event package from the non-controlling MCPTT function as specified in subclause 10.1.3.4.3 and the non-controlling MCPTT function subscribes to the conference state event package from the controlling MCPTT function as specified in subclause 10.1.3.5.3.

10.1.3.2 MCPTT client

A MCPTT client may subscribe to the conference state event package when a group call is ongoing and the ongoing group call is not initiated as a broadcast group call by sending a SIP SUBSCRIBE request to obtain information of the status of a group session.

When subscribing to the conference state event package, the MCPTT client:

1) shall generate a SIP SUBSCRIBE request and use a new SIP-dialog according to IETF RFC 6665 [26], IETF RFC 4575 [30] and 3GPP TS 24.229 [4];

2) shall set the Request-URI of the SIP SUBSCRIBE request to the MCPTT session identity of the group session;

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-Preferred-Service header field according to IETF RFC 6050 [9];

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

5) if the MCPTT client wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295;

NOTE 1: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

6) if the MCPTT client wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [26], to zero;

7) shall include an Accept header field containing the application/conference-info+xml"MIME type;

8) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcptt-request-uri> element set to the MCPTT group ID of the group session; and

9) shall send the SIP SUBSCRIBE request using a new SIP dialog according to 3GPP TS 24.229 [4].

The responses to the SIP SUBSCRIBE request shall be handled according to IETF RFC 6665 [26], IETF RFC 4575 [30] and TS 24.229 [4].

Upon receiving a SIP NOTIFY requests to the previously sent SIP SUBSCRIBE request the MCPTT client:

1) shall handle the request according to IETF RFC 6665 [26] and IETF RFC 4575 [30]; and

2) may display the current state information to the MCPTT client based on the information in the SIP NOTIFY request body.

When needed the MCPTT client shall terminate the subscription and indicate it terminated according to IETF RFC 6665 [26].

NOTE 2: The contents of the received SIP NOTIFY request body is specified in subclause 6.3.3.4.

10.1.3.3 Participating MCPTT function

Upon receipt of a SIP SUBSCRIBE request for conference event status subscription from a MCPTT user served by the participating MCPTT function and if the SIP SUBSCRIBE request contains:

1) 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 header field according to IETF RFC 6050 [9];

2) an Accept header field containing the application/conference-info+xml"MIME type; and

3) an application/vnd.3gpp.mcptt-info+xml MIME body containing the <mcptt-request-uri> set to a MCPTT group ID;

then the participating MCPTT function:

1) shall attempt to resolve the received Request-URI to an existing MCPTT session identity;

2) if the participating MCPTT function could not resolve the received Request-URI to an existing MCPTT session identity, shall reject the SIP SUBSCRIBE response with a SIP 404 (Not Found) response with a warning text set to "137 the indicated group call does not exists" as specified in subclause 4.4 and shall skip the rest of the steps

3) shall generate a SUBSCRIBE request as specified in TS 24.229 [4]

4) shall set the SIP URI in the Request-URI with the MCPTT session identity that is mapped to the MCPTT session identity in the received Request-URI;

5) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body the <mcptt-calling-user-id> element set to the MCPTT ID of the served user: and

6) shall insert a Record-Route header containing a URI identifying its own address; and

7) shall send the SIP SUBSCRIBE request according to 3GPP TS 24.229 [4].

Upon receiving a SIP response to the SIP SUBSCRIBE request the participating MCPTT function:

1) shall copy the content of the incoming SIP response to an outgoing SIP response;

2) if a SIP 200 (OK) response, shall include in the Contact header field of the outgoing SIP response an MCPTT session identity mapped to the MCPTT session identity provided in the Contact header field of the received SIP 200 (OK) response in the outgoing SIP response; and

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

Upon receiving a SIP NOTIFY request within the dialog created by the SIP SUBSCRIBE request destined to a served MCPTT client, the participating MCPTT function:

1) shall include the public service identity of the MCPTT user in the Request-URI;

2) shall copy the content of the incoming SIP NOTIFY request to the outgoing SIP NOTIFY request; and

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

Upon receiving a SIP response to the SIP NOTIFY request the participating MCPTT function:

1) shall copy the content of the incoming SIP response to an outgoing SIP response;

2) if a SIP 200 (OK) response, shall include an MCPTT session identity constructed from the MCPTT session identity provided in the Contact header field of the received SIP 200 (OK) response in the outgoing SIP response; and

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

10.1.3.4 Controlling MCPTT function

10.1.3.4.1 Receiving a subscription to the conference event package

Upon receipt of a SIP SUBSCRIBE request for event package subscription in the controlling MCPTT function and the SIP SUBSCRIBE request:

1) contains an application/vnd.3gpp.mcptt-info+xml MIME body with

   a) the <mcptt-request-uri> element set to the group identity of the group session and the <mcptt-calling-user-id> element set to either:

      i) the MCPTT ID of a participant in the group session; or

      ii) a constituent MCPTT group ID of a non-controlling MCPTT function in a temporary group session;

2) contains 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 header field according to IETF RFC 6050 [9];

3) contains an Accept header field containing the application/conference-info+xml MIME type; and

4) is not received in a group call initiated as a broadcast group call;

then the controlling MCPTT function:

1) shall check if the <on-network-allow-conference-state> element in the group document in 3GPP TS 24.481 [31] allows the MCPTT ID or the constituent MCPTT group ID in the <mcptt-calling-user-id> element to subscribe to the conference event package and if not allowed:

   a) shall reject the "SIP SUBSCRIBE request for event status subscription in the controlling MCPTT function" with a SIP 403 (Forbidden) response to the SIP SUBSCRIBE request, with warning text set to "138 subscription of conference events not allowed" as specified in subclause 4.4; and

   b) shall not continue with the remaining steps;

2) shall handle the request according to IETF RFC 6665 [26] and IETF RFC 4575 [30];

3) shall cache information about the subscription;

4) shall send a conference state notification as specified in subclause 10.1.3.4.2; and

5) if the SIP SUBSCRIBE request is the first SUBSCRIBE request from a participant in a temporary group session, shall subscribe to the conference event package from all non-controlling MCPTT functions in the group session as specified in subclause 10.1.3.4.3.

Upon receipt of a SIP SUBSCRIBE request for event package subscription in the controlling MCPTT function in an group call initiated as a broadcast group call, the controlling MCPTT function:

1) shall generate a SIP 480 (Temporarily Unavailable) response to the SIP SUBSCRIBE request as specified in 3GPP TS 24.229 [4];

2) shall include a Warning header field with the warning text set to "105 subscription not allowed in a broadcast group call" as specified in subclause 4.4; and

3) send the SIP 480 (Temporarily Unavailable) response according to 3GPP TS 24.229 [4].

10.1.3.4.2 Sending notifications to the conference event package

The procedures in this subclause is triggered by:

1) the receipt of a SIP SUBSCRIBE request as specified in subclause 10.1.3.4.1;

2) the receipt of a SIP BYE request from one of the participants in a pre-arranged or a chat group session; or

3) when a new participant is added in a pre-arranged or chat group session.

When sending a conference state event notification, the controlling MCPTT function:

1) shall generate a notification package as specified in subclause 6.3.3.4 to all MCPTT clients which have subscribed to the conference state event package; and

NOTE: As a group document can potentially have a large content, the controlling MCPTT function can notify using content-indirection as defined in IETF RFC 4483 [32].

2) shall send a SIP NOTIFY request to all participants which have subscribed to the conference state event package as specified in 3GPP TS 24.229 [4].

10.1.3.4.3 Sending subscriptions to the conference event package

The procedure in this subclause is triggered by:

1) the receipt of a SIP 200 (OK) response to a SIP INVITE request for non-controlling MCPTT function of an MCPTT group and if at least one participant already has subscribed to the conference event package in the controlling MCPTT function as specified in subclause 10.1.3.4.1; or

2) the receipt of the first SIP SUBSCRIBE request as specified in subclause 10.1.3.4.1 and one or more participant in the group session is a non-controlling MCPTT function;

then, for each non-controlling MCPTT function from where a SIP 200 (OK) response to a SIP INVITE request for non-controlling MCPTT function of an MCPTT group has been received and where a SIP SUBSCRIBE request is not already sent, the controlling MCPTT function:

1) shall generate a SIP SUBSCRIBE request and use a new SIP-dialog according to IETF RFC 6665 [26], IETF RFC 4575 [30] and 3GPP TS 24.229 [4];

2) shall set the Request-URI of the SIP SUBSCRIBE request 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 include the same P-Asserted-Identity header field as included in the SIP INVITE request for non-controlling MCPTT function of an MCPTT group;

4) 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-Preferred-Service header field according to IETF RFC 6050 [9];

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

6) shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295;

NOTE: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

7) shall include an Accept header field containing the application/conference-info+xml MIME type;

8) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with:

   a) the <mcptt-request-uri> element set to the constituent MCPTT group ID; and

   b) the <mcptt-calling-group-id> set to the temporary MCPTT group ID; and

9) shall send the SIP SUBSCRIBE request using a new SIP dialog according to 3GPP TS 24.229 [4].

The responses to the SIP SUBSCRIBE request shall be handled according to IETF RFC 6665 [26], IETF RFC 4575 [30] and TS 24.229 [4].

Upon receiving an incoming SIP NOTIFY requests to the previously sent SIP SUBSCRIBE request, the controlling MCPTT function:

1) shall handle the request according to IETF RFC 6665 [26] and IETF RFC 4575 [30];

2) shall modify the SIP NOTIFY request as specified in subclause 6.3.3.4; and

3) shall forward the modified SIP NOTIFY request according to 3GPP TS 24.229 [4] to all other participants with a subscription to the conference event package.

NOTE: A non-controlling MCPTT function of an MCPTT group is regarded as a participant in a temporary group session.

10.1.3.4.4 Terminating a subscription

Upon receipt of a SIP SUBSCRIBE request for event status subscription in the controlling MCPTT function that terminates the subscription of the conference event package as specified in IETF RFC 6665 [26], the controlling MCPTT function:

1) shall send a SIP 200 (OK) response as specified in IETF RFC 6665 [26]; and

2) if there are no remaining subscriptions to the event package in the ongoing MCPTT call in a temporary group session, shall terminate the subscriptions to the conference event package as specified in IETF RFC 6665 [26] in all non-controlling MCPTT functions in the temporary group session.

Upon expiry of the subscription timer and if there are no remaining subscriptions to the event package in the ongoing MCPTT call in a temporary group session, the controlling MCPTT function shall terminate the subscriptions to the conference event package as specified in IETF RFC 6665 [26] in all non-controlling MCPTT functions in the temporary group session.

10.1.3.5 Non-controlling MCPTT function

10.1.3.5.1 Receiving subscriptions to the conference event package

Upon receipt of SIP SUBSCRIBE request for event package subscription in the non-controlling MCPTT function and the SIP SUBSCRIBE request:

1) contains an application/vnd.3gpp.mcptt-info+xml MIME body with

   a) the <mcptt-request-uri> element set to the constituent MCPTT group ID; and

   b) the <mcptt-calling-user-id> element is set to:

      i) a participant in the group session; or

      ii) the temporary MCPTT group ID;

2) contains 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 header field according to IETF RFC 6050 [9];

3) contains an Accept header field containing the application/conference-info+xml MIME type; and

4) is not received in a group call initiated as a broadcast group call;

then the non-controlling MCPTT function:

1) shall check if the <on-network-allow-conference-state> element in the group document in 3GPP TS 24.481 [31] of the constituent group allows the MCPTT ID in the <mcptt-calling-user-id> element to subscribe to the conference event package and if not allowed:

   a) shall reject the "SIP SUBSCRIBE request for event status subscription in the controlling MCPTT function" with a SIP 403 (Forbidden) response to the SIP SUBSCRIBE request, with warning text set to "138 subscription of conference events not allowed" as specified in subclause 4.4; and

   b) shall not continue with the remaining steps;

2) shall handle the request according to IETF RFC 6665 [26] and IETF RFC 4575 [30];

3) shall cache information about the subscription;

4) shall generate a notification package as specified in subclause 6.3.4.3 and send a SIP NOTIFY request according to 3GPP TS 24.229 [4] to the MCPTT client which have subscribed to the conference state event; and

5) if the SIP SUBSCRIBE request is the first SIP SUBSCRIBE request from a MCPTT client, shall subscribe to the conference event package from the controlling MCPTT functions in the group session as specified in subclause 10.1.3.5.3.

Upon receipt of a SIP SUBSCRIBE request for event package subscription in the controlling MCPTT function in a group call initiated as a broadcast group call, the controlling MCPTT function:

1) shall generate a SIP 480 (Temporarily Unavailable) response to the SIP SUBSCRIBE request as specified in 3GPP TS 24.229 [4];

2) shall include a Warning header field with the warning text set to "105 subscription not allowed in a broadcast group call" as specified in subclause 4.4; and

3) send the SIP 480 (Temporarily Unavailable) response according to 3GPP TS 24.229 [4].

10.1.3.5.2 Sending notifications to the conference event package

The procedures in this subclause is triggered by:

1) the receipt of a receipt of a SIP BYE request from one of the participants in a pre-arranged or a chat group session; or

2) when a new participant is added in a pre-arranged or chat group session.

When sending a conference state event notification, the non-controlling MCPTT function:

1) shall generate a notification package as specified in subclause 6.3.4.3 to all participants which have subscribed to the conference state event package; and

NOTE: As a group document can potentially have a large content, the controlling MCPTT function can notify using content-indirection as defined in IETF RFC 4483 [32].

2) shall send a SIP NOTIFY request to all participants which have subscribed to the conference state event package as specified in 3GPP TS 24.229 [4].

10.1.3.5.3 Sending a subscription to the conference event package

Upon receipt of the first subscription to the conference event package from an MCPTT client, the non-controlling MCPTT function:

1) shall generate a SIP SUBSCRIBE request and use a new SIP-dialog according to IETF RFC 6665 [26], IETF RFC 4575 [30] and 3GPP TS 24.229 [4];

2) shall set the Request-URI of the SIP SUBSCRIBE request to the temporary MCPTT session identity;

NOTE: The SIP URI received in the Contact header field of the SIP INVITE request for non-controlling MCPTT function of an MCPTT group is the temporary MCPTT session identity. Towards MCPTT clients the non-controlling MCPTT function uses an internal generated MCPTT session identity.

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 header field according to IETF RFC 6050 [9];

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

5) shall set the Expires header field according to IETF RFC 6665 [26], to 4294967295;

NOTE 2: 4294967295, which is equal to 2^{32}-1, is the highest value defined for Expires header field in IETF RFC 3261 [24].

6) shall include an Accept header field containing the application/conference-info+xml MIME type;

7) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with:

   a) the <mcptt-request-uri> element set to the temporary MCPTT group ID: and

   b) the <mcptt-calling-group-id> set to the constituent MCPTT group ID; and

8) shall send the SIP SUBSCRIBE request using a new SIP dialog according to 3GPP TS 24.229 [4].

The 2xx response to the SIP SUBSCRIBE request shall be handled according to IETF RFC 6665 [26], IETF RFC 4575 [30] and TS 24.229 [4].

Upon receiving an incoming SIP NOTIFY requests to the previously sent SIP SUBSCRIBE request the non-controlling MCPTT function:

1) shall handle the request according to IETF RFC 6665 [26] and IETF RFC 4575 [30];

2) shall store conference information based on the SIP NOTIFY request content;

3) shall modify the SIP NOTIFY request as specified in subclause 6.3.4.3; and

4) forward the modified SIP NOTIFY request according to 3GPP TS 24.229 [4] to all MCPTT clients with a subscription to the conference event package.

10.1.3.5.4 Terminating a subscription

Upon receipt of a SIP SUBSCRIBE request for event status subscription in the non-controlling MCPTT function that terminates the subscription of the conference event package as specified in IETF RFC 6665 [26], the non-controlling MCPTT function:

1) shall send a SIP 200 (OK) response as specified in IETF RFC 6665 [26]; and

2) if there are no remaining subscriptions to the event package (excluding any subscriptions to the event package made by the controlling MCPTT function), shall terminate the subscriptions to the conference event package in the controlling MCPTT function as specified in IETF RFC 6665 [26].

Upon expiry of the subscription timer and if there are no remaining subscriptions to the event package (excluding any subscriptions to the event package made by the controlling MCPTT function), the non-controlling MCPTT function shall terminate the subscriptions to the conference event package in the controlling MCPTT function as specified in IETF RFC 6665 [26].

NOTE: The subscription to the event package made by the controlling MCPTT function will be terminated by the controlling MCPTT function when the last subscription to the event package is terminated in the controlling MCPTT function.

10.1.4 Remote change of an MCPTT user's selected group

10.1.4.1 General

Subclause 10.1.4 specifies the MCPTT client procedures, participating MCPTT function procedures and controlling MCPTT function procedures for the on-network remote change of an MCPTT user's selected group.

10.1.4.2 Client procedures

10.1.4.2.1 Remote selected group change initiation

Upon receiving a request from the MCPTT user to send a group selection change request to change the selected group of a targeted MCPTT user to a specific MCPTT group, the MCPTT client:

1) if:

   a) the <RemoteGroupSelectionURIList> element does not exist in the MCPTT user profile document with one or more <entry> elements (see the MCPTT user profile document in 3GPP TS 24.484 [50]); or

   b) the <RemoteGroupSelectionURIList> element exists in the MCPTT user profile document and the MCPTT ID of the targeted MCPTT user does not match with one of the <entry> elements of the <RemoteGroupSelectionURIList> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]);

   then:

   a) should indicate to the requesting MCPTT user that they are not authorised to change the selected MCPTT group of the targeted MCPTT user; and

   b) shall skip the rest of the steps of the present subclause;

2) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] with the following clarifications:

   a) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP MESSAGE request;

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

   c) may include a P-Preferred-Identity header field in the SIP MESSAGE request containing a public user identity as specified in 3GPP TS 24.229 [4]; and

   d) shall include an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <anyExt> element containing:

      i) the <mcptt-request-uri> set to the MCPTT group identity to be selected by the targeted MCPTT user; and

      ii) the <request-type> element set to a value of "group-selection-change-request"; and

   e) shall insert in the SIP MESSAGE request a MIME resource-lists body with the MCPTT ID of the targeted MCPTT user, according to rules and procedures of IETF RFC 5366 [20];

3) shall set the Request-URI to the public service identity identifying the participating MCPTT function serving the MCPTT user; and

4) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request, should indicate to the MCPTT user the failure of the sent group selection change request and not continue with the rest of the steps.

Upon receiving a "SIP MESSAGE request for group selection change response for terminating client", the MCPTT client:

1) shall determine the success or failure of the sent group selection change request from the value of the <selected-group-change-outcome> element contained in the <anyExt> element of the <mcptt-Params> element of the <mcpttinfo> element of the application/vnd.3gpp.mcptt-info+xml MIME body included in the received SIP MESSAGE request; and

2) should indicate to the MCPTT user the success or failure of the sent group selection change request.

10.1.4.2.2 Target client procedures for handling remote selected group change request

Upon receiving a "SIP MESSAGE request for group selection change request for terminating client", the MCPTT client:

1) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcptt-info+xml MIME body containing an <affiliation-required> element set to a value of "true":

   a) shall invoke the procedures of subclause 9.2.1.2 to affiliate to the MCPTT group identified by the contents of the <mcptt-calling-group-id> included in the application/vnd.3gpp.mcptt-info+xml MIME body;

   b) if the MCPTT client has not already invoked the procedures of subclause 9.2.1.3, shall invoke the procedures of subclause 9.2.1.3; and

   c) upon receiving a SIP NOTIFY request including a <p-id> element set to a value matching the <p-id> value included in the SIP PUBLISH request sent in step 1) a) above as specified in subclause 9.2.1.3, shall determine if the affiliation procedure to the MCPTT group identified by the contents of the <mcptt-calling-group-id> in the received SIP MESSAGE request was successful;

   2) if the received SIP MESSAGE request contained an application/vnd.3gpp.mcptt-info+xml MIME body containing an <affiliation-required> element set to a value of "true" and the affiliation was successful as determined in step 1) c) above, or if the <affiliation-required> element was not present in the received SIP MESSAGE request:

   a) shall change the MCPTT client's selected group to the MCPTT group identified by the contents of the <mcptt-request-uri> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body included in the received SIP MESSAGE request; and

   b) shall determine the success or failure of the change of selected group action;

3) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] with the following clarifications:

   a) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP MESSAGE request;

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

   c) may include a P-Preferred-Identity header field in the SIP MESSAGE request containing a public user identity as specified in 3GPP TS 24.229 [4]; and

   d) shall include in an application/resource-lists+xml MIME body, the MCPTT ID contained in the <mcptt-calling-user-id> element in the application/ vnd.3gpp.mcptt-info+xml MIME body of the received SIP MESSAGE request;

   e) shall include an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <anyExt> element containing:

      i) the <response-type> element set to a value of "group-selection-change-response";

      ii) the <mcptt-request-uri> set to the MCPTT group identity to be selected by the MCPTT user;

iii) if the MCPTT client was able to successfully change the selected group as determined in step 2) b) above, include a <selected-group-change-outcome> element set to a value of "success"; or

iv) if the MCPTT client:

A) was required to affiliate to the MCPTT group identified by the contents of the <mcptt-calling-group-id> in the received SIP MESSAGE request and the affiliation failed as determined in step 1) c); or

B) failed to change the selected group as determined in step 2) b)

then include a <selected-group-change-outcome> element set to a value of "fail";

4) should indicate to the MCPTT user the success or failure of the requested change of selected group action;

5) shall set the Request-URI to the public service identity identifying the participating MCPTT function serving the MCPTT user; and

6) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

10.1.4.3 Participating MCPTT function procedures

10.1.4.3.1 Originating procedures

Upon receiving a "SIP MESSAGE request for group-selection-change for originating 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 MESSAGE 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 skip the rest of the steps;

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

NOTE: 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 the "SIP MESSAGE request for group selection change for originating participating MCPTT function" contains the <request-type> element set to a value of "group-selection-change-request":

a) if:

i) the <RemoteGroupSelectionURIList> element does not exist in the MCPTT user profile document with one or more <entry> elements (see the MCPTT user profile document in 3GPP TS 24.484 [50]); or

ii) if the MCPTT ID contained in the <mcptt-request-uri> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body included in the received "SIP MESSAGE request for group selection change for originating participating MCPTT function" does not match with one of the <entry> elements of the <RemoteGroupSelectionURIList> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]);

then:

i) shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "155 user not authorised to change user's selected group" 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 determine the public service identity of the controlling MCPTT function associated with the group identity contained in the <mcptt-request-uri> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body;

5) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

6) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the controlling MCPTT function associated with the group identity contained in the received SIP MESSAGE request;

7) shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP MESSAGE request into an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 included in the outgoing SIP MESSAGE request;

8) shall copy the contents of the application/resource-lists MIME body into the outgoing SIP MESSAGE request;

9) shall set the <mcptt-calling-user-id> element of the <mcpttinfo> element containing the <mcptt-Params> element to the MCPTT ID determined in step 2) above;

10) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP MESSAGE request;

11) 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];

12) 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];

13) 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 MESSAGE request; and

14) shall send the SIP MESSAGE request as specified to 3GPP TS 24.229 [4].

Upon receipt of a SIP 2xx response in response to the sent SIP MESSAGE request, the participating MCPTT function shall generate a SIP 200 (OK) response and forward the SIP 200 (OK) response to the MCPTT client.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request, shall forward the error response to the MCPTT client.

10.1.4.3.2 Terminating procedures

Upon receiving a "SIP MESSAGE request for group-selection-change 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 MESSAGE 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 skip the rest of the steps;

2) 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 MESSAGE request to retrieve the binding between the MCPTT ID and public user identity;

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

4) shall generate an outgoing SIP MESSAGE request as specified in subclause 6.3.2.2.11;

5) 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 MESSAGE request; and

6) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the participating MCPTT function shall forward the SIP 2xx response to the controlling MCPTT function.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request, shall forward the response to the controlling MCPTT function.

10.1.4.4 Controlling MCPTT function procedures

Upon receiving:

- a "SIP MESSAGE request for group selection change request for controlling MCPTT function"; or
- a "SIP MESSAGE request for group selection change response for controlling MCPTT function";

the controlling 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 MESSAGE request with a SIP 500 (Server Internal Error) response. The controlling 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;

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

3) if there is a <request-type> element set to a value of "group-selection-change-request" contained in the <anyExt> element in the <mcptt-Params> element contained in the <mcpttinfo> root element contained in the application/vnd.3gpp. mcptt-info+xml MIME body in the received SIP MESSAGE request:

   a) if the MCPTT user identified by the MCPTT ID in the application/resource-lists MIME body contained in the SIP MESSAGE request is not affiliated with the MCPTT group identified by the <mcptt-request-uri> in the application/vnd.3gpp. mcptt-info+xml MIME body as determined by the procedures of subclause 6.3.6:

      i) shall determine if the MCPTT user is eligible to be affiliated with the MCPTT group as determined by subclause 9.2.2.3.8; and

      ii) if the MCPTT user is not eligible for affiliation, shall reject the SIP MESSAGE request with 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;

4) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

5) 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];

6) 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];

7) shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP MESSAGE request into an application/vnd.3gpp.mcptt-info+xml MIME body included in the outgoing SIP MESSAGE request with the following clarifications:

   a) shall set the <mcptt-calling-group-id> to the MCPTT group identity contained in the <mcptt-request-uri> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body included in the received SIP MESSAGE request; and

   b) shall set the <mcptt-request-uri> element of the application/vnd.3gpp. mcptt-info+xml MIME body in the outgoing SIP MESSAGE request to the MCPTT ID of the targeted MCPTT user contained in the application/resource-lists MIME body contained in the received SIP MESSAGE request;

8) if the received SIP MESSAGE request is a "SIP MESSAGE request for group selection change request for controlling MCPTT function":

   a) if the targeted MCPTT user is not affiliated to the identified MCPTT group and was determined to be eligible to be affiliated with the MCPTT group in step 3) a) i) above, shall include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <anyExt> element an <affiliation-required> element set to a value of "true";

9) shall set the Request-URI to the public service identity of the terminating participating MCPTT function associated with the targeted MCPTT user;

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

10) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

11) shall copy the public user identity of the calling MCPTT user from the P-Asserted-Identity header field of the incoming SIP MESSAGE request into the P-Asserted-Identity header field of the outgoing SIP MESSAGE request; and

12) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [4].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the controlling MCPTT function shall generate a SIP 200 (OK) response and forward the SIP 200 (OK) response to the originating participating MCPTT function.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request, controlling MCPTT function shall forward the error response to the originating participating MCPTT function.

10.2 Off-network group call

10.2.1 General

10.2.1.1 Common Procedures

10.2.1.1.1 MONP message transport

In order to participate in a call of an MCPTT group, the MCPTT client:

1) shall send the MONP message as a UDP message to the multicast IP address of the MCPTT group, on UDP port TBD, with an IP time-to-live set to 255; and

Editor's note [CT1#95-bis, C1-160770]: Port number for the message is FFS.

2) shall treat UDP messages received on the multicast IP address of the MCPTT group and on port TBD as received MONP messages.

The MONP message is the entire payload of the UDP message.

10.2.1.1.2 Session description

For an off-network MCPTT session, only MCPTT speech is used.

One off-network MCPTT session includes one media-floor control entity.

The MCPTT client shall generate an SDP body for a group call in accordance with rules and procedures of RFC4566 [12].

The MCPTT client:

1) shall include in the session-level section:

   a) the "o=" field with the <username> portion set to a dash;

   b) the "s=" field with the <session name> portion set to a dash; and

   c) the "c=" field with the <nettype> portion set to "IN", the <addrtype> portion set to the IP version of a multicast IP address of the MCPTT group and the <connection-address> portions set to the multicast IP address of the MCPTT group;

2) shall include the media-level section for MCPTT speech consisting of:

   a) the "m=" field with the <media> portion set to "audio", the <port> portion set to a port number for MCPTT speech of the MCPTT group, the <proto> field set to "RTP/AVP" and <fmt> portion set indicating RTP payload type numbers;

   b) the "i=" field with the <session description> portion set to "speech";

c) the "a=fmtp:" attribute(s), the "a=rtpmap:" attribute(s) or both, indicating the codec(s) and media parameters of the MCPTT speech with the following clarification:

i) if the "/<x>/<x>/Common/PreferredVoiceCodec" leaf node is present in the group document configured on the group management client as specified in 3GPP TS 24.483 [45] containing an RTP payload format name as specified in IETF RFC 4566 [12], indicating a preferred voice codec for an MCPTT group; and

ii) if the MCPTT client supports the encoding name indicated in the value of the "name" attribute;

then the MCPTT client:

i) shall insert the value of the "/<x>/<x>/Common/PreferredVoiceCodec" leaf node in the <encoding name> field of the "a=rtpmap" attribute as defined in IETF RFC 4566 [12]; and

d) the "a=rtcp:" attribute indicating port number to be used for RTCP at the MCPTT client selected according to the rules and procedures of IETF RFC 3605 [13], if the media steam uses other than the default IP address; and

3) shall include the media-level section for media-floor control entity consisting of:

a) an "m=" line, with the <media> portion set to "application", the <port> portion set to a port number for media-floor control entity of the MCPTT group, the <proto> field set to "udp" and <fmt> portion set to "MCPTT"; and

b) the "a=fmtp:MCPTT" attribute indicating the parameters of the media-floor control entity as specified 3GPP TS 24.380 [5].

10.2.2 Basic call control

10.2.2.1 General

In this release of specification, media streams of off-network group call cannot be modified and the SDP is the same for the entire duration of the call.

The maximum number of simultaneous off-network group calls is limited by the value of "/<*x*>/Common/MCPTTGroupCall/MaxCallN4" leaf node present in the UE configuration as specified in 3GPP TS 24.483 [45].

10.2.2.2 Basic call control state machine

The Figure 10.2.2.2-1 gives an overview of the main states and transitions on the UE for call control.

Each call control state machine is per MCPTT group ID.

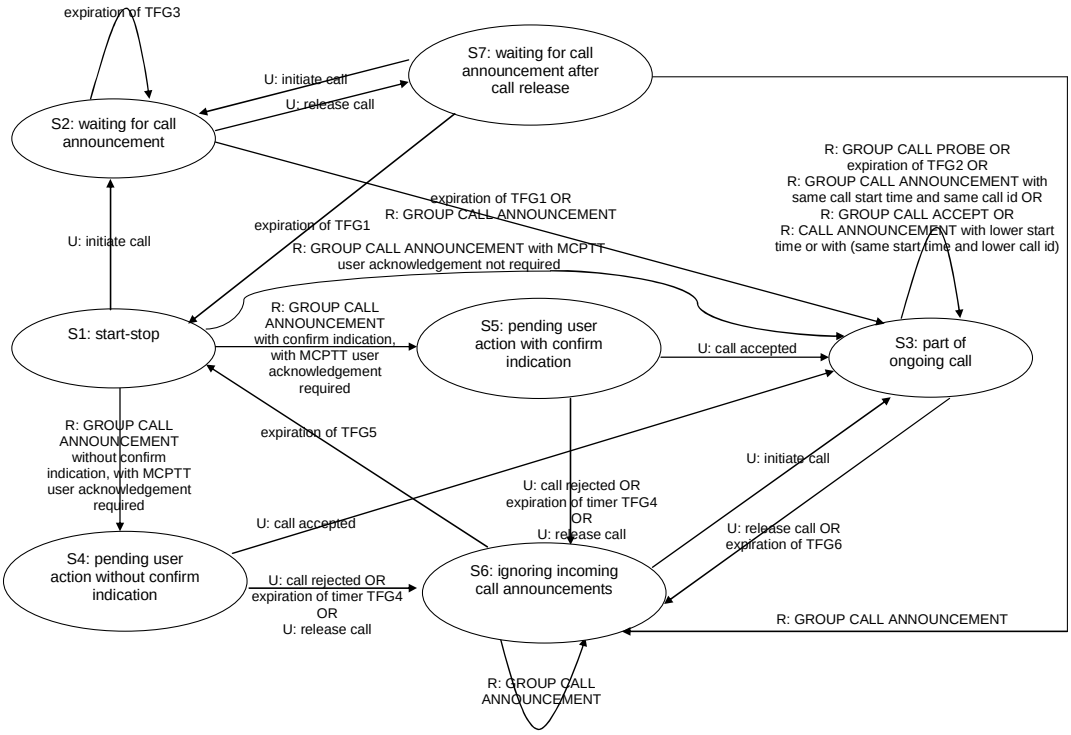

Figure 10.2.2.2-1: Basic call control state machine

The following pieces of information are associated with the basic call control state machine:

a) the stored call identifier of the call;

b) the probe response value of the call;

c) the stored refresh interval of the call;

d) the stored SDP body of the call;

e) the stored originating MCPTT user ID of the call;

f) the stored MCPTT group ID of the call; and

h) the stored call start time of the call.

The basic call control state machine has a related call type control state machine described in subclause 10.2.3.2.

When sending the message, MCPTT client indicates the stored current ProSe per-packet priority associated with the call type control state machine to the lower layers.

10.2.2.3 Call Control states

10.2.2.3.1 S1: start-stop

This state exists for UE, when the UE is not part of an ongoing call.

This state is the start state of this state machine.

This state is the stop state of this state machine.

10.2.2.3.2 S2: waiting for call announcement

This state exists for UE, when the UE has sent a GROUP CALL PROBE message and is waiting for a GROUP CALL ANNOUNCEMENT message.

10.2.2.3.3 S3: part of ongoing call

This state exists for UE, when the UE is part of an ongoing group call.

10.2.2.3.4 S4: pending user action without confirm indication

This state exists for UE, when the UE has presented a notification to the MCPTT user for the received GROUP CALL ANNOUNCEMENT message, is waiting for a response and is not expected to send confirm indication.

10.2.2.3.5 S5: pending user action with confirm indication

This state exists for UE, when the UE has presented a notification to the MCPTT user for the received GROUP CALL ANNOUNCEMENT message, is waiting for a response and is expected to send confirm indication.

10.2.2.3.6 S6: ignoring incoming call announcements

This state exists for UE, when the group call was rejected or released, GROUP CALL ANNOUNCEMENT message was sent or received and GROUP CALL ANNOUNCEMENT messages continue being received.

10.2.2.3.7 S7: waiting for call announcement after call release

This state exists for UE, when the group call was released, GROUP CALL ANNOUNCEMENT message was neither sent nor received and GROUP CALL PROBE was sent.

10.2.2.4 Procedures

10.2.2.4.1 General

10.2.2.4.1.1 Call announcement timer calculation

10.2.2.4.1.1.1 Periodic call announcement timer calculation

The MCPTT client:

1) shall generate a random number, X, with uniform distribution between 0 and 1; and
2) shall set the TFG2 (periodic announcement) timer as follows:
   - TFG2 (periodic announcement) = the refresh interval of the call * (2/3 + 2/3*X) seconds.

10.2.2.4.1.1.2 Call announcement timer calculation after CALL PROBE

The MCPTT client:

1) shall generate a random number, X, with uniform distribution between 0 and 1; and
2) shall set the TFG2 (periodic announcement) timer as follows:
   - TFG2 (periodic announcement) = 1/12*X seconds.

10.2.2.4.1.2 Max duration timer calculation

The MCPTT client shall set the TFG6 (max duration) timer as follows:

- TFG6 (max duration) = X – (Y – Z) seconds, where:

- X = value of "/<*x*>/<x>/OffNetwork/MaxDuration" leaf node present in group configuration as specified in 3GPP TS 24.483 [45];
- Y = current UTC time, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds);
- Z = Call start time IE of the GROUP CALL ANNOUNCEMENT message.

10.2.2.4.2 Call Probe

10.2.2.4.2.1 Call probe initiation

When in the "S1: start-stop" state, upon an indication from an MCPTT user to initiate a group call for an MCPTT group ID, the MCPTT client:

1) shall store the MCPTT group ID as the MCPTT group ID of the call;
2) shall create a call type control state machine as described in subclause 10.2.3.2;
3) shall generate a GROUP CALL PROBE message as specified in subclause 15.1.2. In the GROUP CALL PROBE message, the MCPTT client:
   a) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call;
4) shall send the GROUP CALL PROBE message as specified in subclause 10.2.1.1.1;
5) shall start timer TFG3 (call probe retransmission);
6) shall start timer TFG1 (wait for call announcement); and
7) shall enter the "S2: waiting for call announcement" state.

10.2.2.4.2.2 Call probe retransmission

When in the "S2: waiting for call announcement" state, upon expiration of TFG3 (call probe retransmission), the MCPTT client:

1) shall generate a GROUP CALL PROBE message as specified in subclause 15.1.2. In the GROUP CALL PROBE message, the MCPTT client:
   a) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call;
2) shall send the GROUP CALL PROBE message as specified in subclause 10.2.1.1.1;
3) shall start timer TFG3 (call probe retransmission); and
4) shall remain in the "S2: waiting for call announcement" state.

10.2.2.4.2.3 Receiving GROUP CALL PROBE message when participating in the ongoing call

When in the "S3: part of ongoing call" state, upon receiving a GROUP CALL PROBE message with the MCPTT group ID IE matching the stored MCPTT group ID of the call, the MCPTT client:

1) if the stored probe response value of the call is set to "false":
   a) shall stop timer TFG2 (call announcement);
   b) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.2; and
   c) shall set the stored probe response of the call to "true"; and
2) shall remain in the "S3: part of ongoing call" state.

10.2.2.4.3 Call setup

10.2.2.4.3.1 Not receiving any response to GROUP CALL PROBE message

When in the "S2: waiting for call announcement" state, upon expiry of timer TFG1 (wait for call announcement), the MCPTT client:

1) shall stop timer TFG3 (call probe retransmission), if running;
2) shall generate an SDP body as specified in subclause 10.2.1.1.2 and store it as the SDP body of the call;
3) shall generate a random number with uniform distribution between 0 and 65535 and store it as the call identifier of the call;
4) shall select refresh interval value and store it as the refresh interval of the call;
5) shall store own MCPTT user ID as the originating MCPTT user ID of the call;
6) shall store the current UTC time as the call start time of the call;
7) shall generate a GROUP CALL ANNOUNCEMENT message as specified in subclause 15.1.3. In the GROUP CALL ANNOUNCEMENT message, the MCPTT client:
   a) shall set the Call identifier IE to the stored call identifier of the call;
   b) shall set the Call type IE to the stored current call type associated with the call type control state machine;
   c) shall set the Refresh interval IE to the stored refresh interval of the call;
   d) shall set the SDP IE to the stored SDP body of the call;
   e) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call;
   f) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call;
   g) shall set the Call start time IE to the stored call start time of the call;
   h) shall set the Last call type change time IE to the stored last call type change time of the call associated with call type control state machine;
   i) shall set the Last user to change call type IE to last user to change call type associated with call type control state machine; and
   j) may include the Confirm mode indication IE;
8) shall send the GROUP CALL ANNOUNCEMENT message as specified in subclause 10.2.1.1.1;
9) shall establish a media session based on the stored SDP body of the call;
10) shall start floor control as originating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];
11) shall start timer TFG6 (max duration) with value as specified in subclause 10.2.2.4.1.2;
12) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.1; and
13) shall enter the "S3: part of ongoing call" state.

Note: In this release of the specification, the refresh interval of the call is fixed to 10 seconds.

10.2.2.4.3.2 Receiving a GROUP CALL ANNOUNCEMENT message

When in the "S2: waiting for call announcement" state, upon receiving a GROUP CALL ANNOUNCEMENT message with the MCPTT group ID IE matching the stored MCPTT group ID of the call, the MCPTT client:

1) shall stop timer TFG3 (call probe retransmission);
2) shall stop timer TFG1 (wait for call announcement);

3) shall store the value of the SDP IE of the GROUP CALL ANNOUNCEMENT message as the SDP body of the call;

4) shall store the value of the Call identifier IE of the GROUP CALL ANNOUNCEMENT message as the call identifier of the call;

5) shall store the value of the originating MCPTT user ID IE of the GROUP CALL ANNOUNCEMENT message as the Originating MCPTT user ID of the call;

6) shall store the value of the Refresh interval IE of the GROUP CALL ANNOUNCEMENT message as the refresh interval of the call;

7) shall store the value of the Call start time IE of the GROUP CALL ANNOUNCEMENT message as the call start time of the call;

8) shall establish a media session based on the stored SDP body of the call;

9) shall start floor control as terminating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];

10) shall start timer TFG6 (max duration) with value as specified in subclause 10.2.2.4.1.2;

11) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.1; and

12) shall enter the "S3: part of ongoing call" state.

10.2.2.4.3.3 Receiving a GROUP CALL ANNOUNCEMENT message when not participating in the ongoing call

When in the "S1: start-stop" state, upon receiving a GROUP CALL ANNOUNCEMENT message with the MCPTT group ID IE not matching MCPTT group ID of the call stored for other state machines, the MCPTT client:

1) shall store the value of the SDP IE of the GROUP CALL ANNOUNCEMENT message as the SDP body of the call;

2) shall store the value of the Call identifier IE of the GROUP CALL ANNOUNCEMENT message as the call identifier of the call;

3) shall store the value of the Originating MCPTT user ID IE of the GROUP CALL ANNOUNCEMENT message as the originating MCPTT user ID of the call;

4) shall store the value of the Refresh interval IE of the GROUP CALL ANNOUNCEMENT message as the refresh interval of the call;

5) shall store the value of the MCPTT group ID IE of the GROUP CALL ANNOUNCEMENT message as the MCPTT group ID of the call;

6) shall store the value of the Call start time IE of the GROUP CALL ANNOUNCEMENT message as the call start time of the call;

7) shall create a call type control state machine as described in subclause 10.2.3.2;

8) if the terminating UE is configured that the terminating MCPTT user acknowledgement is required upon a terminating call request reception:

   a) shall start timer TFG4 (waiting for the user);

   b) if the GROUP CALL ANNOUNCEMENT message contains the Confirm mode indication IE, shall enter the "S5: pending user action with confirm indication" state; and

   c) if the GROUP CALL ANNOUNCEMENT message does not contains the Confirm mode indication IE, shall enter the "S4: pending user action without confirm indication" state; and

9) if the terminating UE is configured that the terminating MCPTT user acknowledgement is not required upon a terminating call request reception:

   a) shall establish a media session based on the stored SDP body of the call;

b) shall start floor control as terminating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];

c) if the GROUP CALL ANNOUNCEMENT message contains the Confirm mode indication IE:

i) shall generate a GROUP CALL ACCEPT message as specified in subclause 15.1.4. In the GROUP CALL ACCEPT message, the MCPTT client:

A) shall set the Call identifier IE to the stored call identifier of the call;

B) shall set the Sending MCPTT user ID IE to own MCPTT user id;

C) shall set the Call type IE to the stored current call type associated with the call type control state machine; and

D) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call; and

ii) shall send the GROUP CALL ACCEPT message as specified in subclause 10.2.1.1.1;

d) shall start timer TFG6 (max duration) with value as specified in subclause 10.2.2.4.1.2;

e) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.1; and

f) shall enter the "S3: part of ongoing call" state.

10.2.2.4.3.4 MCPTT user accepts the terminating call with confirm indication

When in the "S5: pending user action with confirm indication" state, upon indication from the MCPTT user to accept the incoming group call, the MCPTT client:

1) shall establish a media session based on the stored SDP body of the call;

2) shall start floor control as terminating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];

3) shall generate a GROUP CALL ACCEPT message as specified in subclause 15.1.4. In the GROUP CALL ACCEPT message, the MCPTT client:

a) shall set the Call identifier IE to the stored call identifier of the call;

b) shall set the Sending MCPTT user ID IE to own MCPTT user id;

c) shall set the Call type IE to the stored current call type associated with the call type control state machine; and

d) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call; and

4) shall send the GROUP CALL ACCEPT message as specified in subclause 10.2.1.1.1;

5) shall start timer TFG6 (max duration) with value as specified in subclause 10.2.2.4.1.2;

6) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.1; and

7) shall enter the "S3: part of ongoing call" state.

10.2.2.4.3.5 MCPTT user accepts the terminating call without confirm indication

When in the "S4: pending user action without confirm indication" state, upon an indication from the MCPTT user to accept the incoming group call, the MCPTT client:

1) shall establish a media session based on the stored SDP body of the call;

2) shall start floor control as terminating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];

3) shall start timer TFG6 (max duration) with value as specified in subclause 10.2.2.4.1.2;

4) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.1; and

5) shall enter the "S3: part of ongoing call" state.

10.2.2.4.3.6 Receiving GROUP CALL ACCEPT message

When in the "S3: part of ongoing call" state, upon receiving a GROUP CALL ACCEPT message with the MCPTT group ID IE matching the stored MCPTT group ID of the call, the MCPTT client:

1) can inform the MCPTT user about the call acceptance; and
2) shall remain in the "S3: part of ongoing call" state.

10.2.2.4.3.7 MCPTT user rejects the terminating call

When in the "S5: pending user action with confirm indication" state or the "S4: pending user action without confirm indication" state, upon an indication from the MCPTT user to reject the incoming group call, the MCPTT client:

1) shall stop timer TFG4 (waiting for the user);
2) shall start timer TFG5 (not present incoming call announcements); and
3) shall enter the "S6: ignoring incoming call announcements" state.

10.2.2.4.3.8 MCPTT user does not act on terminating call

When in the "S5: pending user action with confirm indication" state or the "S4: pending user action without confirm indication" state, upon expiration of timer TFG4 (waiting for the user), the MCPTT client:

1) shall start timer TFG5 (not present incoming call announcements); and
2) shall enter the "S6: ignoring incoming call announcements" state.

10.2.2.4.4 Periodic group call announcement

10.2.2.4.4.1 Sending periodic call announcement

When in the "S3: part of ongoing call" state, upon expiry of timer TFG2 (call announcement), the MCPTT client:

1) shall generate a GROUP CALL ANNOUNCEMENT message as specified in subclause 15.1.3. In the GROUP CALL ANNOUNCEMENT message, the MCPTT client:
   a) shall set the Call identifier IE to the stored call identifier of the call;
   b) shall set the Call type IE to the stored current call type associated with the call type control state machine;
   c) shall set the Refresh interval IE to the stored refresh interval of the call;
   d) shall set the SDP IE to the stored SDP body of the call;
   e) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call;
   f) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call;
   g) shall set the Last call type change time IE to the stored last call type change time of the call associated with call type control state machine;
   h) shall set the Last user to change call type IE to last user to change call type associated with call type control state machine;
   i) shall set the Call start time IE to the stored call start time of the call;
   j) if the stored probe response value of the call is set to "true", shall include Probe response IE;
2) shall send the GROUP CALL ANNOUNCEMENT message as specified in subclause 10.2.2.1.1.1;
3) if the stored probe response value of the call is set to "true", shall set the stored probe response value of the call to "false";
4) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.1; and

5) shall remain in the "S3: part of ongoing call" state.

10.2.2.4.4.2 Receiving periodic call announcement

When in the "S3: part of ongoing call" state, upon receiving a GROUP CALL ANNOUNCEMENT message with the MCPTT group ID IE matching the stored MCPTT group ID of the call, the Call start time IE being the same as the stored call start time of the call, the Last call type change time IE being the same as the stored last call type change time of the call associated with the call type control state machine, the Last user to change call type IE being the same as the stored last user to change call type of the call associated with the call type control state machine and the Call identifier IE being the same as the stored call identifier of the call and Call type IE same as the stored current call type associated with the call type control state machine and:

1) if the stored probe response value of the call is set to "true" and GROUP CALL ANNOUNCEMENT message contains Probe response IE; or

2) if the stored probe response value of the call is set to "false":

the MCPTT client,

1) shall stop timer TFG2 (call announcement);

2) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.1;

3) shall set the stored probe response of the call to "false", if set to "true"; and

4) shall remain in the "S3: part of ongoing call" state.

10.2.2.4.5 Call release

10.2.2.4.5.1 MCPTT user leaves the call when GROUP CALL ANNOUNCEMENT was sent or received

When in the "S3: part of ongoing call" state, the "S5: pending user action with confirm indication" state, or the "S4: pending user action without confirm indication" state, upon an indication from the MCPTT user to release the group call, the MCPTT client:

1) shall release the media session, if established;

2) shall stop floor control as specified in subclause 7.2.3.9.2 in 3GPP TS 24.380 [5];

3) shall stop timer TFG4 (waiting for the user), if running;

4) shall stop timer TFG2 (call announcement), if running;

5) shall start timer TFG5 (not present incoming call announcements);

6) shall stop timer TFG6 (max duration); and

7) shall enter the "S6: ignoring incoming call announcements" state.

10.2.2.4.5.2 Receiving GROUP CALL ANNOUNCEMENT message for rejected or released call

When in the "S6: ignoring incoming call announcements" state, upon receiving a GROUP CALL ANNOUNCEMENT message with the MCPTT group ID IE matching the stored MCPTT group ID of the call, the MCPTT client:

1) shall store the value of the SDP IE of the GROUP CALL ANNOUNCEMENT message as the SDP body of the call;

2) shall store the value of the Call identifier IE of the GROUP CALL ANNOUNCEMENT message as the call identifier of the call;

3) shall store the value of the Originating MCPTT user ID IE of the GROUP CALL ANNOUNCEMENT message as the originating MCPTT user ID of the call;

4) shall store the value of the Refresh interval IE of the GROUP CALL ANNOUNCEMENT message as the refresh interval of the call;

5) shall store the value of the Call start time IE of the GROUP CALL ANNOUNCEMENT message as the call start time of the call;

6) shall stop timer TFG5 (not present incoming call announcements);

7) shall start timer TFG5 (not present incoming call announcements); and

8) shall remain in the "S6: ignoring incoming call announcements" state.

10.2.2.4.5.3 MCPTT user initiates originating call for rejected or released call

When in the "S6: ignoring incoming call announcements" state, upon an indication from the MCPTT user to initiate a group call for an MCPTT group ID matching the stored MCPTT group ID of the call, the MCPTT client:

1) stop timer TFG5 (not present incoming call announcements);

2) shall establish a media session based on the stored SDP body of the call;

3) shall start floor control as terminating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];

4) shall start timer TFG6 (max duration) with value as specified in subclause 10.2.2.4.1.2;

5) shall start timer TFG2 (call announcement) with value as specified in subclause 10.2.2.4.1.1.1; and

6) shall enter the "S3: part of ongoing call" state.

10.2.2.4.5.4 No GROUP CALL ANNOUNCEMENT messages for rejected or released call

When in the "S6: ignoring incoming call announcements" state, upon expiration of timer TFG5 (not present incoming call announcements), the MCPTT client:

1) shall release the stored SDP body of the call;

2) shall release the stored call identifier of the call;

3) shall release the stored originating MCPTT user ID of the call;

4) shall release the stored refresh interval of the call;

5) shall release the stored MCPTT group ID of the call;

6) shall release the call start time of the call;

7) shall destroy the call type control state machine as specified in subclause 10.2.3.4.10 or 10.2.3.4.11; and

8) shall enter the "S1: start-stop" state.

10.2.2.4.5.5 MCPTT user leaves the call when GROUP CALL PROBE was sent

When in the "S2: waiting for call announcement" state, upon an indication from the MCPTT user to release the group call, the MCPTT client:

1) shall stop timer TFG3 (call probe retransmission); and

2) shall enter the "S7: Waiting for call announcement after call release" state.

10.2.2.4.5.6 MCPTT user initiates originating call for released call

When in the "S7: Waiting for call announcement after call release" state, upon an indication from the MCPTT user to initiate a group call for an MCPTT group ID matching the stored MCPTT group ID of the call, the MCPTT client:

1) shall stop timer TFG1 (wait for call announcement);

2) shall generate a GROUP CALL PROBE message as specified in subclause 15.1.2. In the GROUP CALL PROBE message, the MCPTT client:

   a) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call; and

3) shall send the GROUP CALL PROBE message as specified in subclause 10.2.1.1.1;

4) shall start timer TFG3 (call probe retransmission);

5) shall start timer TFG1 (wait for call announcement); and

6) shall enter the "S2: waiting for call announcement" state.

10.2.2.4.5.7 Receiving GROUP CALL ANNOUNCEMENT message for released call

When in the "S7: Waiting for call announcement after call release" state, upon receiving a GROUP CALL ANNOUNCEMENT message with the MCPTT group ID IE matching the stored MCPTT group ID of the call, the MCPTT client:

1) shall store the value of the SDP IE of the GROUP CALL ANNOUNCEMENT message as the SDP body of the call;

2) shall store the value of the Call identifier IE of the GROUP CALL ANNOUNCEMENT message as the call identifier of the call;

3) shall store the value of the Originating MCPTT user ID IE of the GROUP CALL ANNOUNCEMENT message as the originating MCPTT user ID of the call;

4) shall store the value of the Refresh interval IE of the GROUP CALL ANNOUNCEMENT message as the refresh interval of the call;

5) shall store the value of the Call start time IE of the GROUP CALL ANNOUNCEMENT message as the call start time of the call;

6) shall stop timer TFG1 (wait for call announcement);

7) shall start timer TFG5 (not present incoming call announcements); and

8) shall enter the "S6: ignoring incoming call announcements" state.

10.2.2.4.5.8 No GROUP CALL ANNOUNCEMENT messages for released call

When in the "S7: Waiting for call announcement after call release" state, upon expiration of timer TFG1 (wait for call announcement), the MCPTT client:

1) shall release the stored MCPTT group ID of the call;

2) shall destroy the call type control state machine as specified in subclause 10.2.3.4.11; and

3) shall enter the "S1: start-stop" state.

10.2.2.4.5.9 Max duration reached

When in the "S3: part of ongoing call" state, upon expiration of timer TFG6 (max duration), the MCPTT client:

1) shall release the media session;

2) shall stop floor control as specified in subclause 7.2.3.9.2 in 3GPP TS 24.380 [5];

3) shall stop timer TFG2 (call announcement), if running;

4) shall start timer TFG5 (not present incoming call announcements); and

5) shall enter the "S6: ignoring incoming call announcements" state.

10.2.2.4.6 Merge of calls

10.2.2.4.6.1 Merge of two calls

When in the "S3: part of ongoing call" state, upon receiving a GROUP CALL ANNOUNCEMENT message with the MCPTT group ID IE matching the stored MCPTT group ID of the call and:

1) the Originating MCPTT user ID IE is different from the stored originating MCPTT user ID of the call; or

2) the Call identifier IE is different from the stored call identifier of the call;

then:

1) if the stored current call type associated with the call type control state machine is "BASIC GROUP CALL" and the value of the Call type IE of GROUP CALL ANNOUNCEMENT message is either "IMMINENT PERIL GROUP CALL" or "EMERGENCY GROUP CALL";

2) if the stored current call type associated with the call type control state machine is "IMMINENT PERIL GROUP CALL" and the value of the Call type IE of GROUP CALL ANNOUNCEMENT message is "EMERGENCY GROUP CALL";

3) if the stored current call type associated with the call type control state machine being equal to the Call type IE of the GROUP CALL ANNOUNCEMENT message and the Call start time IE of the GROUP CALL ANNOUNCEMENT message being lower than the stored call start time of the call; or

4) if the stored current call type associated with the call type control state machine being equal to the Call type IE of the GROUP CALL ANNOUNCEMENT message and the Call start time IE of the GROUP CALL ANNOUNCEMENT message being equal to the stored call start time of the call and the Call identifier IE of the GROUP CALL ANNOUNCEMENT message being lower than the stored call identifier of the call;

the MCPTT client:

1) shall store the value of the SDP IE of the GROUP CALL ANNOUNCEMENT message as the SDP body of the call;

2) shall store the value of the Call identifier IE of the GROUP CALL ANNOUNCEMENT message as the call identifier of the call;

3) shall store the value of the Originating MCPTT user ID IE of the GROUP CALL ANNOUNCEMENT message as the originating MCPTT user ID of the call;

4) shall store the value of the Refresh interval IE of the GROUP CALL ANNOUNCEMENT message as the refresh interval of the call;

5) shall store the value of the Call start time IE of the GROUP CALL ANNOUNCEMENT message as the call start time of the call;

6) shall adjust the media session based on the stored SDP body of the call and restart floor control as terminating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];

7) shall stop timer TFG6 (max duration);

8) shall start timer TFG6 (max duration) with value as specified in subclause 10.2.2.4.1.2;

9) shall stop timer TFG2 (call announcement); and

10) shall start timer TFG2 (call announcement) with value according to rules and procedures as specified in subclause 10.2.2.4.1.1.1; and

11) shall remain in the "S3: part of ongoing call" state.

10.2.2.4.7 Error handling

10.2.2.4.7.1 Unexpected MONP message received

Upon receiving a MONP message in a state where there is no handling specified for the MONP message, the MCPTT client shall discard the MONP message.

10.2.2.4.7.2 Unexpected indication from MCPTT user

Upon receiving an indication from the MCPTT user in a state where there is no handling specified for the indication, the MCPTT client shall ignore the indication.

10.2.2.4.7.3 Unexpected expiration of a timer

Upon expiration of a timer in a state where there is no handling specified for expiration of the timer, the MCPTT client shall ignore the expiration of the timer.

10.2.3. Call type control

10.2.3.1 General

This state machine exists in parallel with the basic call control state machine for off-network group call as specified in subclause 10.2.2.2.

10.2.3.2 Call type control state machine

The Figure 10.2.3.2-1 gives an overview of the states and transitions of the state machine.

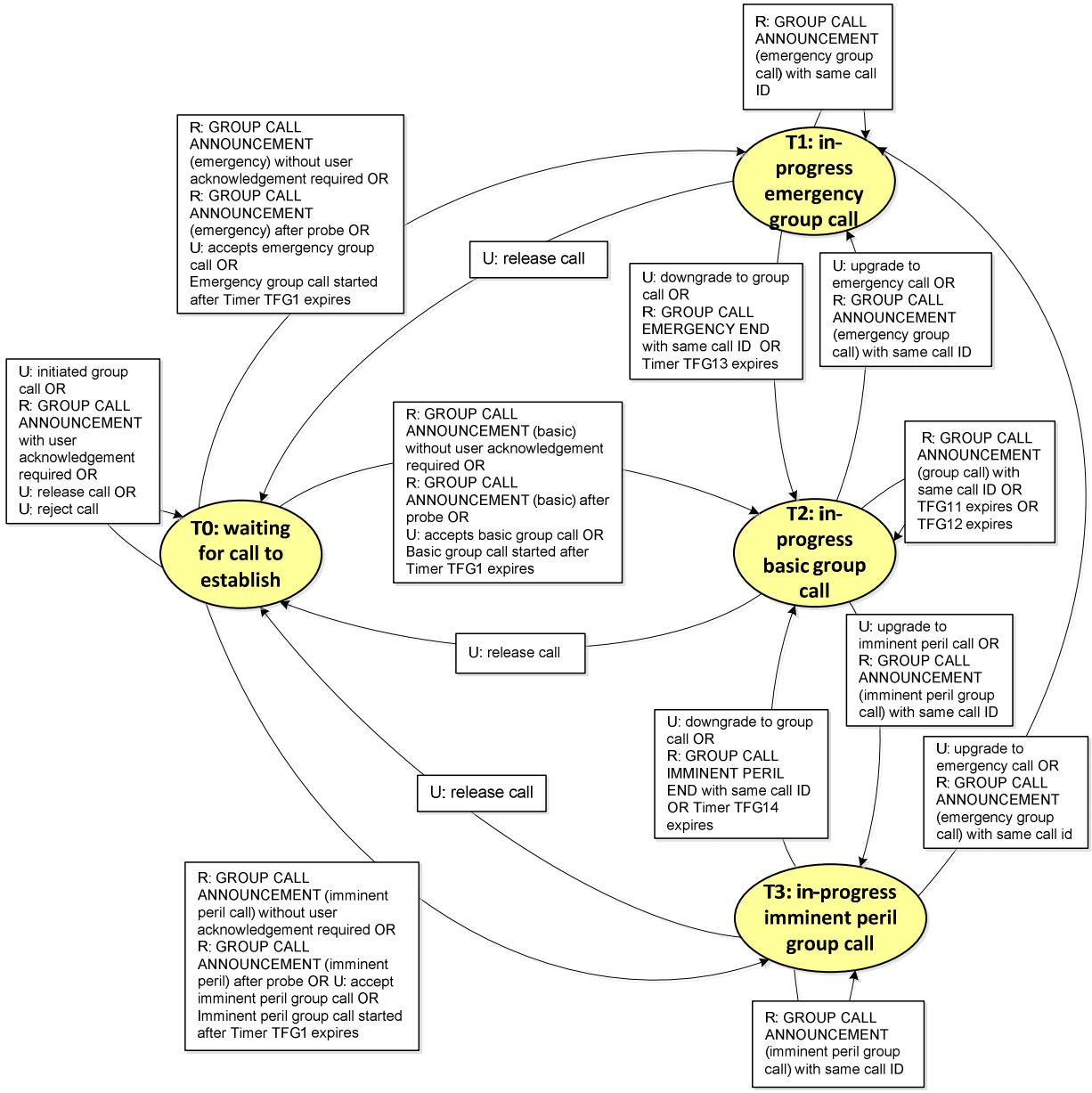

Figure 10.2.3.2-1: Call type control state machine

The following pieces of information are associated with the call type control state machine:

a) the stored current call type;

b) the stored current ProSe per-packet priority;

c) the stored last call type change time of the call; and

d) the stored last user to change call type of the call.

When sending the message, MCPTT client indicates the stored current ProSe per-packet priority (as described in 3GPP TS 24.483 [45]) associated with the call type control state machine to the lower layers.

10.2.3.3 Call type control states

10.2.3.3.1 T0: waiting for call to establish

This state is the start state of this state machine.

10.2.3.3.2 T1: in-progress emergency group call

This state exists for UE, when the UE is part of an in-progress emergency group call.

10.2.3.3.3 T2: in-progress basic group call

This state exists for UE, when the UE is part of an in-progress basic group call.

10.2.3.3.4 T3: in-progress imminent peril group call

This state exists for UE, when the UE is part of an in-progress imminent peril group call.

10.2.3.4 Procedures

10.2.3.4.1 General

10.2.3.4.1.1 Implicit downgrade (emergency) timer calculation

The MCPTT client shall set the TFG13 (implicit downgrade emergency) timer as follows:

1) TFG13 (implicit downgrade emergency) = X – (Y – Z) seconds, where:

   a) X = value of "/<x>/<x>/OffNetwork/EmergencyCallCancel" leaf node present in group configuration as specified in 3GPP TS 24.483 [45];

   b) Y = current UTC time, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds); and

   c) Z = Last call type change time IE of the GROUP CALL ANNOUNCEMENT message or the Last call type change time IE of the GROUP CALL PRIORITY ENDED message.

10.2.3.4.1.2 Implicit downgrade (imminent peril) timer calculation

The MCPTT client shall set the TFG14 (implicit downgrade imminent peril) timer as follows:

1) TFG14 (implicit downgrade imminent peril) = X – (Y – Z) seconds, where:

   a) X = value of "/<x>/<x>/OffNetwork/ImminentPerilCallCancel" leaf node present in group configuration as specified in 3GPP TS 24.483 [45];

   b) Y = current UTC time, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds); and

   c) Z = Last call type change time IE of the GROUP CALL ANNOUNCEMENT message or the Last call type change time IE of the GROUP CALL PRIORITY ENDED message.

10.2.3.4.2 User initiated the call probe

When in the "T0: waiting for the call to establish " state, upon an indication from an MCPTT user to initiate a group call probe for an MCPTT group, the MCPTT client:

1) if the stored emergency state associated with emergency alert state machine described in 12.2.2.2 is set to "true" and the value of "/<*x*>/<x>/Common/AllowedEmergencyCall" leaf node present in group configuration as specified in 3GPP TS 24.483 [45] is set to "true":

   a) shall set the stored current call type to "EMERGENCY GROUP CALL"; and

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

2) if the stored emergency state associated with emergency alert state machine described in 12.2.2.2 is set to "false", and:

   a) if the user initiates an MCPTT emergency call and the values of "/<*x*>/<*x*>/Common/MCPTTGroupCall/EmergencyCall/Enabled" leaf node present in the user profile and

"/<*x*>/<x>/Common/AllowedEmergencyCall" leaf node present in group configuration as specified in 3GPP TS 24.483 [45] are set to "true":

i) shall set the stored current call type to "EMERGENCY GROUP CALL"; and

ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

b) if the user initiates an MCPTT imminent peril group call and the values of "/<*x*>/<*x*>/Common/MCPTTGroupCall/ImminentPerilCall/Authorised" leaf node present in the user profile "/<*x*>/<x>/Common/AllowedImminentPerilCall " leaf node present in group configuration as specified in 3GPP TS 24.483 [45] are set to "true":

i) shall set the stored current call type to "IMMINENT PERIL GROUP CALL"; and

ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network imminent peril group call as described in 3GPP TS 24.483 [45]; and

c) if the user initiates an MCPTT group call which is not an MCPTT emergency call and which is not an MCPTT imminent peril group call:

i) shall set the stored current call type to "BASIC GROUP CALL"; and

ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45];

3) shall set the stored last call type change time to current UTC time;

4) shall set the last user to change call type to own MCPTT user ID; and

5) shall remain in "T0: waiting for the call to establish" state.

10.2.3.4.3 Received GROUP CALL ANNOUNCEMENT message as a response to GROUP CALL PROBE message

When in the "T0: waiting for the call to establish " state, upon receipt of a GROUP CALL ANNOUNCEMENT message as a response to GROUP CALL PROBE message, the MCPTT client:

1) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "EMERGENCY GROUP CALL":

a) shall set the stored current call type to "EMERGENCY GROUP CALL";

b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

c) shall set the stored last call type change time to the Last call type change time IE of the GROUP CALL ANNOUNCEMENT message;

d) shall set the stored last user to change call type to the Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message;

d) shall start timer TFG13 (implicit downgrade emergency) with value as specified in subclause 10.2.3.4.1.1; and

e) shall enter "T1: in-progress emergency group call" state;

2) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "IMMINENT PERIL GROUP CALL", and if the stored current call type is other than "EMERGENCY GROUP CALL":

a) shall set the stored current call type to "IMMINENT PERIL GROUP CALL";

b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network imminent peril group call as described in 3GPP TS 24.483 [45];

c) shall set the stored last call type change time to the Last call type change time IE of the GROUP CALL ANNOUNCEMENT message;

d) shall set the stored last user to change call type to the Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message;

e) shall start timer TFG14 (implicit downgrade imminent peril) with value as specified in subclause 10.2.3.4.1.2; and

f) shall enter "T3: in-progress imminent peril group call" state; and

3) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "BASIC GROUP CALL", and if the stored current call type is "BASIC GROUP CALL":

a) shall set the stored last call type change time to the Last call type change time IE of the GROUP CALL ANNOUNCEMENT message;

b) shall set the stored last user to change call type to the Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message; and

c) shall enter "T2: in-progress basic group call" state.

10.2.3.4.4 Received GROUP CALL ANNOUNCEMENT with MCPTT user acknowledgement required

When in the "T0: waiting for the call to establish" state, upon receipt of a GROUP CALL ANNOUNCEMENT message by an idle MCPTT client when MCPTT user acknowledgement is required, the MCPTT client:

1) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "EMERGENCY GROUP CALL":

a) shall set the stored current call type to "EMERGENCY GROUP CALL"; and

b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

2) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "IMMINENT PERIL GROUP CALL":

a) shall set the stored current call type to "IMMINENT PERIL GROUP CALL"; and

b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network imminent peril group call as described in 3GPP TS 24.483 [45];

3) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "BASIC GROUP CALL":

a) shall set the stored current call type to "BASIC GROUP CALL";

b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45];

4) shall set the stored last call type change time to the Last call type change time IE of the GROUP CALL ANNOUNCEMENT message;

5) shall set the last user to change call type to the Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message; and

6) shall remain in "T0: waiting for the call to establish" state.

10.2.3.4.5 Received GROUP CALL ANNOUNCEMENT without MCPTT user acknowledgement required

When in the "T0: waiting for the call to establish" state, upon receipt of a GROUP CALL ANNOUNCEMENT message by an idle MCPTT client when MCPTT user acknowledgement is not required, the MCPTT client:

1) shall set the stored last call type change time to the Last call type change time IE of the GROUP CALL ANNOUNCEMENT message;

2) shall set the last user to change call type to the Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message;

3) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "EMERGENCY GROUP CALL":

   a) shall set the stored current call type to "EMERGENCY GROUP CALL";

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

   c) shall start timer TFG13 (implicit downgrade emergency) with value as specified in subclause 10.2.3.4.1.1; and

   d) shall enter "T1: in-progress emergency group call" state;

4) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "IMMINENT PERIL GROUP CALL":

   a) shall set the stored current call type to "IMMINENT PERIL GROUP CALL";

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network imminent peril group call as described in3GPP TS 24.483 [45];

   c) shall start timer TFG14 (implicit downgrade imminent peril) with value as specified in subclause 10.2.3.4.1.2; and

   d) shall enter "T3: in-progress imminent peril group call" state; and

5) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "BASIC GROUP CALL":

   a) shall set the stored current call type to "BASIC GROUP CALL";

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45]; and

   c) shall enter "T2: in-progress basic group call" state.

10.2.3.4.6 Call started

When in state "T0: waiting for the call to establish", if:

   a) the MCPTT user accepts the call when MCPTT user acknowledgement is required; or

   b) the MCPTT client sends a GROUP CALL ANNOUNCEMENT message on expiry of timer TFG1 (wait for call announcement) associated with the basic call control state machine;

the MCPTT client:

1) if the stored current call type is set to "EMERGENCY GROUP CALL"

   a) shall start timer TFG13 (implicit downgrade emergency) with value as specified in subclause 10.2.3.4.1.1; and

   b) shall enter "T1: in-progress emergency group call" state;

2) if the stored current call type is set to "IMMINENT PERIL GROUP CALL"

   a) shall start timer TFG14 (implicit downgrade imminent peril) with value as specified in subclause 10.2.3.4.1.2; and

   b) shall enter "T3: in-progress imminent peril group call" state; or

3) if the stored current call type is set to "BASIC GROUP CALL"

   a) shall enter "T2: in-progress basic group call" state.

10.2.3.4.7 Upgrade call

10.2.3.4.7.1 Originating user upgrading the call

When in the "T2: in-progress basic group call" state, upon receiving an indication from the user to upgrade the call to "IMMINENT PERIL GROUP CALL" or "EMERGENCY GROUP CALL" or when in the "T3: in-progress imminent peril group call" state, upon receiving an indication from the user to upgrade the call to "EMERGENCY GROUP CALL", the MCPTT client:

1) if the user request is to upgrade the call to "EMERGENCY GROUP CALL" and the value of "/<*x*>/<*x*>/OffNetwork/EmergencyCallChange" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true":

   a) shall set the stored current call type to "EMERGENCY GROUP CALL";

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

   c) shall store the current UTC time as last call type change time of the call;

   d) shall store own MCPTT user ID as last user to change call type of the call;

   e) shall start timer TFG13 (implicit downgrade emergency) with value as specified in subclause 10.2.3.4.1.1;

   f) shall stop timer TFG11 (emergency end retransmission), if running;

   g) shall stop timer TFG14 (implicit downgrade imminent peril), if running; and

   h) shall enter "T1: in-progress emergency group call" state;

2) if the user request is to upgrade the call to "IMMINENT PERIL GROUP CALL" and the value of "/<*x*>/<*x*>/OffNetwork/ ImminentPerilCallChange" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] set to "true":

   a) shall set the stored current call type to "IMMINENT PERIL GROUP CALL";

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network imminent peril group call as described in 3GPP TS 24.483 [45];

   c) shall store the current UTC time as last call type change time of the call;

   d) shall store own MCPTT user ID as last user to change call type of the call;

   e) shall start timer TFG14 (implicit downgrade imminent peril) with value as specified in subclause 10.2.3.4.1.2;

   f) shall stop timer TFG12 (imminent peril end retransmission), if running; and

   g) shall enter "T3: in-progress imminent peril group call" state;

3) shall generate a GROUP CALL ANNOUNCEMENT message as specified in subclause 15.1.3. In the GROUP CALL ANNOUNCEMENT message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier of the call associated with the basic call control state machine;

   b) shall set the Call type IE to the stored current call type;

   c) shall set the Refresh interval IE to the stored refresh interval of the call associated with the basic call control state machine;

   d) shall set the SDP IE to the stored SDP body of the call associated with the basic call control state machine;

e) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call associated with the basic call control state machine;

f) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call associated with the basic call control state machine;

g) shall set the call start time IE to the stored call start time of the call;

h) shall set the Last call type change time IE to the stored last call type change time of the call; and

i) shall set the Last user to change call type IE to the stored last user to change call type of the call; and

4) shall send the GROUP CALL ANNOUNCEMENT message as specified in subclause 10.2.1.1.1;

10.2.3.4.7.2 Terminating UE receiving a GROUP CALL ANNOUNCEMENT message when participating in the ongoing call

When in the "T1: in-progress emergency group call" state or "T2: in-progress basic group call" state or "T3: in-progress imminent peril group call" state, upon receiving a GROUP CALL ANNOUNCEMENT message with the MCPTT group ID IE matching with MCPTT group ID of the ongoing call and the Call Identifier IE being the same as the stored call identifier of the call, the MCPTT client:

1) if the stored last user to change call type of the call is same as the Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message and the stored last call type change time is smaller than Last call type change time IE of the GROUP CALL ANNOUNCEMENT message:

   a) shall set the stored last call type change time of the call to Last call type change time IE of the GROUP CALL ANNOUNCEMENT message;

   b) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "EMERGENCY GROUP CALL" and the stored call type is other than "EMERGENCY GROUP CALL":

      i) shall set the stored current call type to "EMERGENCY GROUP CALL";

      ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

      iii) shall stop timer TFG14 (implicit downgrade imminent peril), if running;

      iv) shall start timer TFG13 (implicit downgrade emergency) with value as specified in subclause 10.2.3.4.1.1; and

      v) shall enter "T1: in-progress emergency group call" state;

   c) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "IMMINENT PERIL GROUP CALL" and the stored call type is other than "IMMINENT PERIL GROUP CALL":

      i) shall set the stored current call type to "IMMINENT PERIL GROUP CALL";

      ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network imminent peril group call as described in 3GPP TS 24.483 [45];

      iii) shall stop timer TFG13 (implicit downgrade emergency), if running;

      iv) shall start timer TFG14 (implicit downgrade imminent peril) with value as specified in subclause 10.2.3.4.1.2; and

      v) shall enter "T3: in-progress imminent peril group call" state; and

   d) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "BASIC GROUP CALL" and the stored call type is other than "BASIC GROUP CALL":

      i) shall set the stored current call type to "BASIC GROUP CALL";

      ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45];

iii) shall stop timer TFG13 (implicit downgrade emergency), if running;

iv) shall stop timer TFG14 (implicit downgrade imminent peril), if running; and

v) shall enter "T2: in-progress basic group call" state; and

2) if the stored last user to change call type of the call is different from the Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message and:

a) if the stored call type is same as Call type IE in the received GROUP CALL ANNOUNCEMENT message and the stored last call type change time is smaller than Last call type change time IE of the GROUP CALL ANNOUNCEMENT message:

i) shall set the stored last call type change time of the call to Last call type change time IE of the GROUP CALL ANNOUNCEMENT message; and

ii) shall set the stored last user to change call type of the call to Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message;

b) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "EMERGENCY GROUP CALL" and the stored call type is other than "EMERGENCY GROUP CALL":

i) shall set the stored last call type change time of the call to Last call type change time IE of the GROUP CALL ANNOUNCEMENT message;

ii) shall set the stored last user to change call type of the call to Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message;

iii) shall set the stored current call type to "EMERGENCY GROUP CALL";

iv) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

v) shall stop timer TFG14 (implicit downgrade imminent peril), if running;

vi) shall start timer TFG13 (implicit downgrade emergency) with value as specified in subclause 10.2.3.4.1.1; and

vii) shall enter "T1: in-progress emergency group call" state; and

c) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "IMMINENT PERIL GROUP CALL" and the stored call type is "BASIC GROUP CALL":

i) shall set the stored last call type change time of the call to Last call type change time IE of the GROUP CALL ANNOUNCEMENT message;

ii) shall set the stored last user to change call type of the call to Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message;

iii) shall set the stored current call type to "IMMINENT PERIL GROUP CALL ";

iv) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network imminent peril group call as described in 3GPP TS 24.483 [45];

v) shall start timer TFG14 (implicit downgrade imminent peril) with value as specified in subclause 10.2.3.4.1.2; and

vi) shall enter "T3: in-progress imminent peril group call" state; and

d) if the Call type IE of the received GROUP CALL ANNOUNCEMENT message is set to "BASIC GROUP CALL" and the stored call type is other than "BASIC GROUP CALL":

i) shall set the stored current call type to "BASIC GROUP CALL";

ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45];

iii) shall stop timer TFG13 (implicit downgrade emergency), if running;

iv) shall stop timer TFG14 (implicit downgrade imminent peril), if running; and

v) shall enter "T2: in-progress basic group call" state.

10.2.3.4.8 Downgrade call

10.2.3.4.8.1 Originating user downgrading emergency group call

When in the "T1: in-progress emergency group call" state, upon receiving an indication from:

1) the MCPTT user who upgraded the MCPTT group call; or

2) an authorized MCPTT user with the value of "/<*x*>/<*x*>/Common/MCPTTGroupCall/EmergencyCall/CancelMCPTTGroup" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true",

to downgrade "EMERGENCY GROUP CALL", the MCPTT client:

1) shall set the stored current call type to "BASIC GROUP CALL";

2) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45];

3) shall set current UTC time as last call type change time of the call;

4) shall store own MCPTT user ID as last user to change call type of the call;

5) shall generate a GROUP CALL EMERGENCY END message as specified in subclause 15.1.15. In the GROUP CALL EMERGENCY END message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier of the call associated with the basic call control state machine;

   b) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call associated with the basic call control state machine;

   c) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call associated with the basic call control state machine;

   d) shall set the Last call type change time IE to the stored last call type change time of the call; and

   e) shall set the Last user to change call type IE to the stored last user to change call type of the call;

6) shall send the GROUP CALL EMERGENCY END message as specified in subclause 10.2.1.1.1;

7) shall stop timer TFG13 (implicit downgrade emergency);

8) shall initialize the counter CFG11 (emergency end retransmission) with value set to 1;

9) shall start timer TFG11 (emergency end retransmission); and

10) shall enter the "T2: in-progress basic group call" state.

10.2.3.4.8.2 Retransmitting GROUP CALL EMERGENCY END

When in the "T2: in-progress basic group call" state, upon expiry of timer TFG11 (emergency end retransmission), the MCPTT client:

1) shall generate a GROUP CALL EMERGENCY END message as specified in subclause 15.1.15. In the GROUP CALL EMERGENCY END message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier of the call associated with the basic call control state machine;

b) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call associated with the basic call control state machine;

c) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call associated with the basic call control state machine;

d) shall set the Last call type change time IE to the stored last call type change time of the call; and

e) shall set the Last user to change call type IE to the stored last user to change call type of the call;

2) shall send the GROUP CALL EMERGENCY END message as specified in subclause 10.2.1.1.1;

3) shall increment the value of the counter CFG11 (emergency end retransmission) by 1;

4) shall start timer TFG11 (emergency end retransmission) if the value of the associated counter CFG11 (emergency end retransmission) is less than the upper limit; and

5) shall remain in "T2: in-progress basic group call" state.

10.2.3.4.8.3 Terminating user downgrading emergency group call

When in the "T1: in-progress emergency group call" state, upon receiving GROUP CALL EMERGENCY END message, the MCPTT client:

1) shall set the stored last call type change time to the Last call type change time IE of the received GROUP CALL EMERGENCY END message;

2) shall set the stored last user to change call type to the Last user to change call type IE of the received GROUP CALL EMERGENCY END message;

3) shall set the stored current call type to "BASIC GROUP CALL";

4) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45];

5) shall stop timer TFG13 (implicit downgrade emergency); and

6) shall enter the "T2: in-progress basic group call" state.

10.2.3.4.8.4 Originating user downgrading imminent peril group call

When in the "T3: in-progress imminent peril group call" state, upon receiving an indication from:

1) the MCPTT user who upgraded the call; or

2) an authorized user with the value of "/<*x*>/<*x*>/Common/MCPTTGroupCall/ImminentPerilCall/Cancel" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true",

to downgrade "IMMINENT PERIL GROUP CALL", the MCPTT client:

1) shall set the stored current call type to "BASIC GROUP CALL";

2) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45];

3) shall set current UTC time as last call type change time of the call;

4) shall store own MCPTT user ID as last user to change call type of the call;

5) shall generate a GROUP CALL IMMINENT PERIL END message as specified in subclause 15.1.14. In the GROUP CALL IMMINENT PERIL END message, the MCPTT client:

a) shall set the Call identifier IE to the stored call identifier of the call associated with the basic call control state machine;

b) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call associated with the basic call control state machine;

c) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call associated with the basic call control state machine;

d) shall set the Last call type change time IE to the stored last call type change time of the call; and

e) shall set the Last user to change call type IE to the stored last user to change call type of the call;

6) shall send the GROUP CALL IMMINENT PERIL END message as specified in subclause 10.2.1.1.1;

7) shall stop timer TFG14 (implicit downgrade imminent peril);

8) shall initialize the counter CFG12 (imminent peril end retransmission) with value set to 1;

9) shall start timer TFG12 (imminent peril end retransmission); and

10) shall enter the "T2: in-progress basic group call" state.

10.2.3.4.8.5 Retransmitting GROUP CALL IMMINENT PERIL END

When in the "T2: in-progress basic group call" state, upon expiry of timer TFG12 (imminent peril end retransmission), the MCPTT client:

1) shall generate a GROUP CALL IMMINENT PERIL END message as specified in subclause 15.1.14. In the GROUP CALL IMMINENT PERIL END message, the MCPTT client:

a) shall set the Call identifier IE to the stored call identifier of the call associated with the basic call control state machine;

b) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call associated with the basic call control state machine;

c) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call associated with the basic call control state machine;

d) shall set the Last call type change time IE to the stored last call type change time of the call; and

e) shall set the Last user to change call type IE to the stored last user to change call type of the call;

2) shall send the GROUP CALL IMMINENT PERIL END message as specified in subclause 10.2.1.1.1;

3) shall increment the value of the counter CFG12 (imminent peril end retransmission) by 1;

4) shall start the timer TFG12 (imminent peril end retransmission) if the value of the associated counter CFG12 (imminent peril end retransmission) is less than the upper limit; and

5) shall remain in "T2: in-progress basic group call" state.

10.2.3.4.8.6 Terminating user downgrading imminent peril group call

When in the "T3: in-progress imminent peril group call" state, upon receiving GROUP CALL IMMINENT PERIL END message, the MCPTT client:

1) shall set the stored last call type change time to the Last call type change time IE of the received GROUP CALL IMMINENT PERIL END message;

2) shall set the stored last user to change call type to the Last user to change call type IE of the received GROUP CALL IMMINENT PERIL END message;

3) shall set the stored current call type to "BASIC GROUP CALL";

4) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45];

5) shall stop timer TFG14 (implicit downgrade imminent peril); and

6) shall enter the "T2: in-progress basic group call" state.

10.2.3.4.8.7 Void

10.2.3.4.8.8 Implicit emergency priority end

When in the "T1: in-progress emergency group call" state, upon expiry of timer TFG13 (implicit downgrade emergency), the MCPTT client:

1) shall store the current UTC time as the stored last call type change time of the call;

2) shall store the originating MCPTT user ID as the stored last user to change call type of the call;

3) shall set the stored current call type to "BASIC GROUP CALL";

4) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45]; and

5) shall enter the "T2: in-progress basic group call" state.

10.2.3.4.8.9 Implicit imminent peril priority end

When in the "T3: in-progress imminent peril call" state, upon expiry of timer TFG14 (implicit downgrade imminent peril), the MCPTT client:

1) shall store the current UTC time as the stored last call type change time of the call;

2) shall store the originating MCPTT user ID as the stored last user to change call type of the call;

3) shall set the stored current call type to "BASIC GROUP CALL";

4) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network basic group call as described in 3GPP TS 24.483 [45]; and

5) shall enter the "T2: in-progress basic group call" state.

10.2.3.4.9 Merge of two calls

When in the "T1: in-progress emergency group call" state or "T2: in-progress basic group call" state or "T3: in-progress imminent peril group call" state, upon receiving a GROUP CALL ANNOUNCEMENT message with the MCPTT group ID IE matching the stored MCPTT group ID of the call and:

1) the Originating MCPTT user ID IE is different from the stored originating MCPTT user ID of the call; or

2) the Call identifier IE is different from the stored call identifier of the call;

then:

1) if the stored current call type is "BASIC GROUP CALL" and the value of the Call type IE of GROUP CALL ANNOUNCEMENT message is either "IMMINENT PERIL GROUP CALL" or "EMERGENCY GROUP CALL"; or

2) if the stored current call type is "IMMINENT PERIL GROUP CALL" and the value of the Call type IE of GROUP CALL ANNOUNCEMENT message is "EMERGENCY GROUP CALL"; or

3) if the stored current call type being equal to the Call type IE of the GROUP CALL ANNOUNCEMENT message and the Call start time IE of the GROUP CALL ANNOUNCEMENT message being lower than the stored call start time of the call; or

4) if the stored current call type being equal to the Call type IE of the GROUP CALL ANNOUNCEMENT message and the Call start time IE of the GROUP CALL ANNOUNCEMENT message being equal to the stored call start time of the call and the Call identifier IE of the GROUP CALL ANNOUNCEMENT message being lower than the stored call identifier of the call;

the MCPTT client:

1) shall store the value of the Last call type change time IE of the received GROUP CALL ANNOUNCEMENT message as the last call type change time of the call;

2) shall store the value of the Last user to change call type IE of the GROUP CALL ANNOUNCEMENT message as the last user to change call type of the call;

3) shall store the value of the Call type IE of the GROUP CALL ANNOUNCEMENT message as the current call type of the call;

4) if the Call type IE of GROUP CALL ANNOUNCEMENT message is set to "EMERGENCY GROUP CALL":

   a) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency group call as described in 3GPP TS 24.483 [45];

   b) shall stop timer TFG14 (implicit downgrade imminent peril), if running;

   c) shall start timer TFG13 (implicit downgrade emergency), if not started already, with values as specified in subclause 10.2.3.4.1.1; and

   d) shall enter "T1: in-progress emergency group call" state; and

5) if the Call type IE of GROUP CALL ANNOUNCEMENT message is set to "IMMINENT PERIL GROUP CALL":

   a) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network imminent peril group call as described in 3GPP TS 24.483 [45];

   b) shall start timer TFG14 (implicit downgrade imminent peril), if not started already, with values as specified in subclause 10.2.3.4.1.2; and

   c) shall enter "T3: in-progress imminent peril group call" state.

10.2.3.4.10 Call release after call establishment

When in state T1: in-progress emergency group call" or "T2: in-progress basic group call" or "T3: in-progress imminent peril group call" or upon receiving an indication from MCPTT user to release the call, the MCPTT client:

1) shall release stored current call type;

2) shall release stored ProSe per-packet priority;

3) shall release Last call type change time;

4) shall release Last user to change call type; and

5) shall enter "T0: waiting for the call to establish" state.

10.2.3.4.11 Call release or reject before call establishment

When in state "T0: waiting for the call to establish", upon receiving an indication from MCPTT user to release or reject the call, the MCPTT client:

1) shall release stored current call type;

2) shall release stored ProSe per-packet priority;

3) shall release Last call type change time;

4) shall release Last user to change call type;

5) shall remain in "T0: waiting for the call to establish" state.

10.2.3.4.12 Error handling

10.2.3.4.12.1 Unexpected MONP message received

Upon receiving a MONP message in a state where there is no handling specified for the MONP message, the MCPTT client shall discard the MONP message.

10.2.3.4.12.2 Unexpected indication from MCPTT user

Upon receiving an indication from the MCPTT user in a state where there is no handling specified for the indication, the MCPTT client shall ignore the indication.

10.2.3.4.12.3 Unexpected expiration of a timer

Upon expiration of a timer in a state where there is no handling specified for expiration of the timer, the MCPTT client shall ignore the expiration of the timer.

10.3 Off-network Broadcast group call

10.3.1 General

10.3.2 Basic call control

10.3.2.1 General

10.3.2.2 Broadcast group call control state machine

The figure 10.3.2.2-1 gives an overview of the main states and transitions on the UE for broadcast group call control.

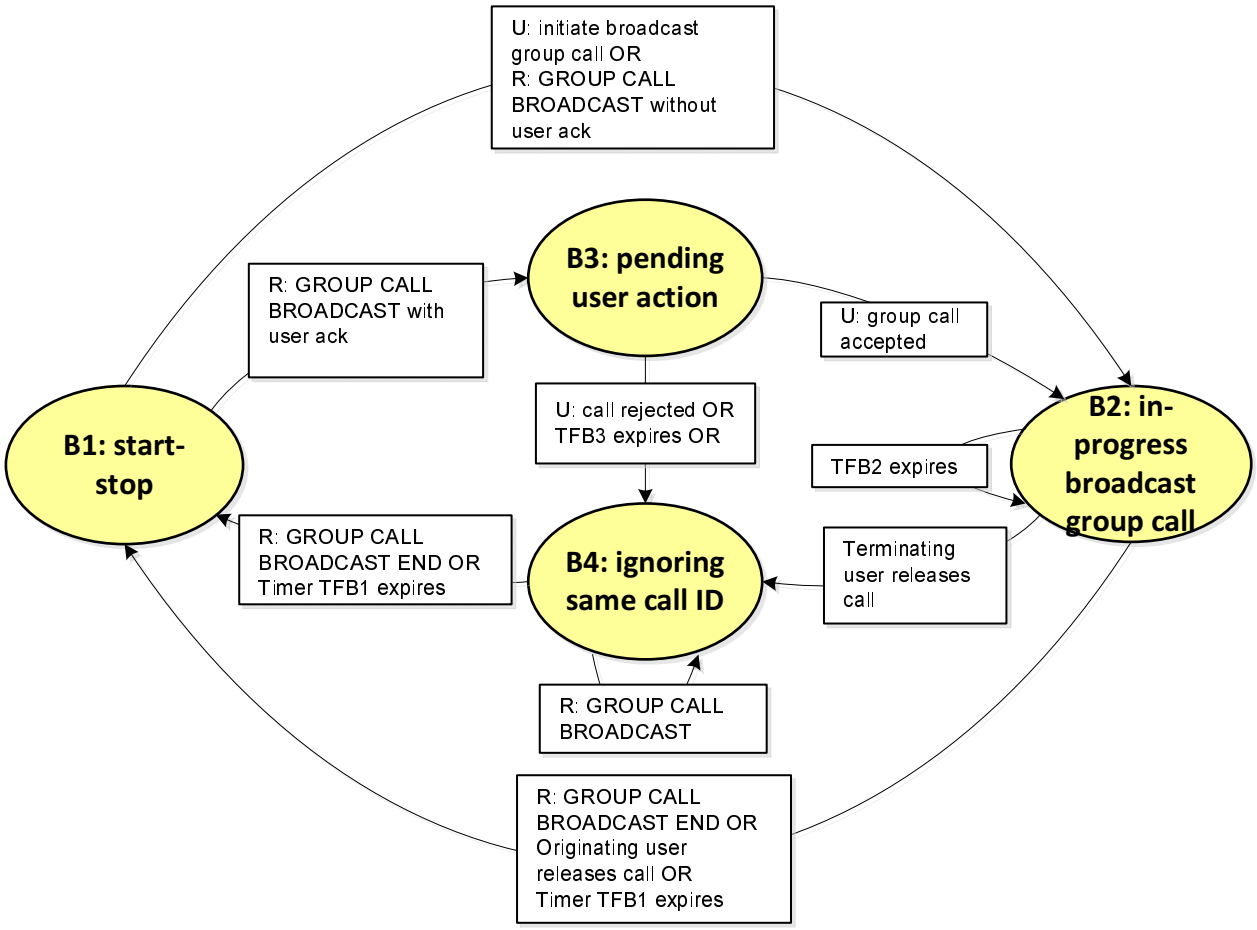

Figure 10.3.2.2-1: Broadcast group call control state machine

10.3.2.3 Broadcast group call Control states

10.3.2.3.1 B1: start-stop

This state exists for UE, when the UE is not part of an ongoing broadcast group call.

10.3.2.3.2 B2: in-progress broadcast group call

This state exists for UE, when the UE is part of an ongoing broadcast group call.

10.3.2.3.3 B3: pending user action

This state exists for the UE, when the UE has presented a notification to the MCPTT user for the received GROUP CALL BROADCAST message, is waiting for a response and is not expected to send confirm indication.

10.3.2.3.4 B4: ignoring same call ID

This state exists for UE, when the group call was rejected or released and GROUP CALL BROADCAST messages continue being received.

10.3.2.4 Procedures

10.3.2.4.1 User initiating a broadcast group call

When in the "B1: start-stop" state, upon the indication from MCPTT user to initiate the broadcast group call, the MCPTT client:

1) shall generate an SDP body as specified in subclause 10.2.1.1.2 and store it as the SDP body of the call;
2) shall generate a random number with uniform distribution between 0 and 65535 and store it as the call identifier of the call;
3) shall store own MCPTT user ID as the originating MCPTT user ID of the call;
4) shall store "BROADCAST GROUP CALL" as the current call type;
5) shall generate a GROUP CALL BROADCAST message as specified in subclause 15.1.20. In the GROUP CALL BROADCAST message, the MCPTT client:
   a) shall set the Call identifier IE to the stored call identifier of the call;
   b) shall set the Call type IE to the stored current call type;
   c) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call;
   d) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call; and
   e) shall set the SDP IE to the stored SDP body of the call;
6) shall set the ProSe per-packet priority to the value corresponding to MCPTT off-network broadcast callas described in 3GPP TS 24.483 [45];
7) shall start floor control as originating floor participant as described specified in subclause 7.2 in 3GPP TS 24.380 [5];
8) shall send the GROUP CALL BROADCAST message as specified in subclause 10.2.1.1.1;
9) shall establish a media session based on the stored SDP body of the call;
10) shall start timer TFB2 (broadcast retransmission); and
11) shall enter the "B2: in-progress broadcast group call" state.

10.3.2.4.2 Terminating UE receiving a GROUP CALL BROADCAST message when not participating in the in-progress broadcast group call

When in the "B1: start-stop" state, upon receiving a GROUP CALL BROADCAST message with the Call identifier IE not matching any in-progress broadcast group call, the MCPTT client:

1) shall store the value of the Call identifier IE of the GROUP CALL BROADCAST message as the call identifier of the call;
2) shall store the value of the Call type IE of the GROUP CALL BROADCAST message as the received current call type;
3) shall store the value of the SDP IE of the GROUP CALL BROADCAST message as the SDP body of the call;
4) shall store the value of the Originating MCPTT user ID IE of the GROUP CALL BROADCAST message as the originating MCPTT user ID of the call;
5) shall store the value of the MCPTT group ID IE of the GROUP CALL BROADCAST message as the MCPTT group ID of the call;
6) if the terminating UE is configured that the terminating MCPTT user acknowledgement is required upon a terminating call request reception:

i) shall start timer TFB3 (waiting for the user); and

ii) shall enter the "B3: pending user action" state; and

7) if the terminating UE is configured that the terminating MCPTT user acknowledgement is not required upon a terminating call request reception:

i) shall establish a media session based on the stored SDP body of the call;

ii) shall start floor control as terminating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];

iii) shall start timer TFB1 (max duration); and

iv) shall enter the "B2: in-progress broadcast group call" state.

10.3.2.4.3 MCPTT user accepts the terminating call

When in the "B3: pending user action" state, upon indication from the MCPTT user to accept the incoming broadcast group call, the MCPTT client:

1) shall establish a media session based on the stored SDP body of the call;

2) shall start floor control as terminating floor participant as described specified in subclause 7.2 in 3GPP TS 24.380 [5];

3) shall stop timer TFB3 (waiting for the user);

4) shall start timer TFB1 (max duration); and

5) shall enter the "B2: in-progress broadcast group call" state.

10.3.2.4.4 MCPTT user rejects the terminating call

When in the "B3: pending user action" state, upon an indication from the MCPTT user to reject the incoming broadcast group call, the MCPTT client:

1) shall stop timer TFB3 (waiting for the user);

2) shall start timer TFB1 (max duration); and

3) shall enter the "B4: ignoring same call ID" state.

10.3.2.4.5 MCPTT user does not act on terminating call

When in the "B3: pending user action" state, upon expiration of timer TFB3 (waiting for the user), the MCPTT client:

1) shall start timer TFB1 (max duration); and

2) shall enter the "B4: ignoring same call ID" state.

10.3.2.4.6 Terminating user releasing the call

When in the "B2: in-progress broadcast group call" state, upon an indication from the terminating MCPTT user to release the in-progress broadcast group call, the MCPTT client:

1) shall release the media session;

2) shall stop floor control; and

3) shall enter the "B4: ignoring same call ID" state.

10.3.2.4.7 Originating user releasing the call

When in the "B2: in-progress broadcast group call" state, upon an indication from the originating MCPTT user to release the in-progress broadcast group call, the MCPTT client:

1) shall release the media session;

2) shall generate a GROUP CALL BROADCAST END message as specified in subclause 15.1.21. In the GROUP CALL BROADCAST END message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier of the call;

   b) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call; and

   c) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call;

3) shall send the GROUP CALL BROADCAST END message as specified in subclause 10.2.1.1.1;

4) shall stop timer TFB2 (broadcast retransmission);

5) shall clear the stored call identifier;

6) shall stop floor control; and

7) shall enter the "B1: start-stop" state.

10.3.2.4.8 Receiving GROUP CALL BROADCAST END message

When in the "B2: in-progress broadcast group call" state or "B4: ignoring same call ID" state, upon receiving GROUP CALL BROADCAST END message with the same Call identifier IE as the stored call identifier, the MCPTT client:

1) shall release media session;

2) shall stop timer TFB1 (max duration);

3) shall clear the stored call identifier;

4) shall stop floor control, if running; and

5) shall enter the "B1: start-stop" state.

10.3.2.4.9 Originating UE retransmitting GROUP CALL BROADCAST message

When in the "B2: in-progress broadcast group call" state, upon expiry of timer TFB2 (broadcast retransmission), the MCPTT client:

1) shall generate a GROUP CALL BROADCAST message as specified in subclause 15.1.20. In the GROUP CALL BROADCAST message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier of the call;

   b) shall set the Call type IE to the stored current call type;

   c) shall set the Originating MCPTT user ID IE to the stored originating MCPTT user ID of the call;

   d) shall set the MCPTT group ID IE to the stored MCPTT group ID of the call; and

   e) shall set the SDP IE to the stored SDP body of the call;

2) shall send the GROUP CALL BROADCAST message as specified in subclause 10.2.1.1.1;

3) shall restart timer TFB2 (broadcast retransmission); and

4) shall remain in the "B2: in-progress broadcast group call" state.

10.3.2.4.10 Ignoring same call ID

When in the "B4: ignoring same call ID" state, upon receiving GROUP CALL BROADCAST message and if the call identifier in GROUP CALL BROADCAST message matches with the stored call identifier the MCPTT client:

1) shall restart timer TFB1 (max duration); and

2) shall remain in "B4: ignoring same call ID" state.

10.3.2.4.11 Releasing the call

When in the "B2: in-progress broadcast group call" state or "B4: ignoring same call ID" state, upon expiry of timer TFB1 (max duration) the MCPTT client:

1) shall release the media session;

2) shall clear the stored call identifier;

3) shall stop floor control, if running; and

4) shall enter the "B1: start-stop" state.

10.3.2.4.12 Restarting TFB1

When in the "B2: in-progress broadcast group call" state, upon receiving GROUP CALL BROADCAST message and if the call identifier in GROUP CALL BROADCAST message matches with the stored call identifier, the MCPTT client:

1) shall restart timer TFB1 (max duration); and

2) shall remain in "B2: in-progress broadcast group call" state.

11 Private call

11.0 General

This subclause describes the private call procedures between two MCPTT clients for on-network and off-network.

For on-network, private call procedures with floor control are specified in subclause 11.1.1 and without floor control are specified in subclause 11.1.2.

For on-network, private call procedures are specified for the MCPTT client, the participating MCPTT function and the controlling MCPTT function on the originating side and terminating side. These procedures include the support for first-to-answer call.

For off-network, only private call procedures with floor control are specified in subclause 11.2.

For off-network, private call procedures are specified for the MCPTT client on the originating side and terminating side.

For both on-network and off-network private calls, the use of automatic commencement mode and manual commencement mode are specified.

11.1 On-network private call and first-to-answer call

11.1.1 Private call with floor control and first-to-answer call with floor control

11.1.1.1 General

Subclause 11.1.1 specifies the MCPTT client procedures, participating MCPTT function procedures and controlling MCPTT function procedures for on-network private calls with floor control and first-to-answer calls with floor control. The procedures cover both on-demand and pre-established session establishment. The procedures also cover emergency private call initiation, upgrade and cancellation.

For a private call, the MCPTT client shall initiate the call to one MCPTT user

For a first-to-answer call, the MCPTT client shall initiate the call to a list of two or more MCPTT users.

11.1.1.2 MCPTT client procedures

11.1.1.2.1 On-demand private call and first-to-answer call

11.1.1.2.1.1 Client originating procedures

Upon receiving a request from an MCPTT user to establish an MCPTT private call the MCPTT client shall generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) shall set the Request-URI of the SIP INVITE request to a public service identity of the participating MCPTT function serving the MCPTT user;

2) if the MCPTT user has requested the origination of a first-to-answer call, if the <allow-request-first-to-answer-call> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false", the MCPTT client shall inform the MCPTT user and shall exit this procedure;

3) if the MCPTT user has requested the origination of an MCPTT emergency private call or is originating an MCPTT private call and the MCPTT emergency state is already set, the MCPTT client:

   a) shall, if this is an authorised request for an MCPTT emergency private call as determined by the procedures of subclause 6.2.8.3.1.1, comply with the procedures in subclause 6.2.8.3.2; and

   b) should, if this is an unauthorised request for an MCPTT emergency private call as determined in step a) above, indicate to the MCPTT user that they are not authorised to initiate an MCPTT emergency private call;

4) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [4];

5) shall include the g.3gpp.mcptt media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

6) 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];

7) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP INVITE request;

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

9) for the establishment of a private call shall insert in the SIP INVITE request a MIME resource-lists body with the MCPTT ID of the invited MCPTT user, according to rules and procedures of IETF RFC 5366 [20];

10) for the establishment of a first-to-answer call shall insert in the SIP INVITE request a MIME resource-lists body with the MCPTT IDs of the potential target MCPTT users, according to rules and procedures of IETF RFC 5366 [20];

11) if an end-to-end security context needs to be established and if the MCPTT user is initiating a private call then:

   a) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [78];

   b) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [78];

   c) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect private call communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [78];

d) shall encrypt the PCK to a UID associated to the MCPTT client using the MCPTT ID and KMS URI of the invited user as determined by the procedures of subclause 6.2.8.3.9 and a time related parameter as described in 3GPP TS 33.180 [78];

e) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [78]; and

g) shall add the MCPTT ID of the originating MCPTT to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]; and

f) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCPTT user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [78];

12) shall include an SDP offer according to 3GPP TS 24.229 [4] with the clarification given in subclause 6.2.1 and with a media stream of the offered media-floor control entity;

13) if implicit floor control is required, shall comply with the conditions specified in subclause 6.4;

14) if the MCPTT user is initiating a private call then:

a) if force of automatic commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include in the SIP INVITE request a Priv-Answer-Mode header field with the value "Auto" according to the rules and procedures of IETF RFC 5373 [18];

b) if force of automatic commencement mode at the invited MCPTT client is not requested by the MCPTT user and:

i) if automatic commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include in the SIP INVITE request an Answer-Mode header field with the value "Auto" according to the rules and procedures of IETF RFC 5373 [18]; and

ii) if manual commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include in the SIP INVITE request an Answer-Mode header field with the value "Manual" according to the rules and procedures of IETF RFC 5373 [18]; and

c) shall contain an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <session-type> element set to a value of "private";

15) if the MCPTT user is initiating a first-to-answer call shall contain an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <session-type> element set to a value of "first-to-answer";

16) if the MCPTT emergency private call state is set to either "MEPC 2: emergency-pc-requested" or "MEPC 3: emergency-pc-granted" or the MCPTT emergency private priority state for this private call is set to "MEPP 2: in-progress", the MCPTT client shall comply with the procedures in subclause 6.2.8.3.3; and

17) shall send SIP INVITE request towards the MCPTT server according to 3GPP TS 24.229 [4].

Upon receiving a SIP 183(Session Progress) response to the SIP INVITE request the MCPTT client:

1) may indicate the progress of the session establishment to the inviting MCPTT user.

Upon receiving a SIP 200 (OK) response to the SIP INVITE request the MCPTT client:

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

2) if the sent SIP INVITE request was for the origination of a first-to-answer call and the SDP answer contained in the received SIP 200 (OK) response contains an "a=key-mgmt" attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

a) shall extract the MCPTT ID of the sender of the SIP 200 (OK) response from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78];

b) shall convert the MCPTT ID to a UID as described in 3GPP TS 33.180 [78];

c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [78];

d) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails:

i) if the sent SIP INVITE request was a request for an MCPTT emergency private call and if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested, the MCPTT client:

A) shall set the MCPTT emergency private call state to "MEPC 1: emergency-pc-capable";

B) if the MCPTT emergency private priority state of the private call is "MEPP 3: confirm-pending" shall set the MCPTT emergency private priority state of the private call to "MEPP 1: no-emergency"; and

C) if the sent SIP request for an MCPTT emergency private call contained an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to a value of "true", shall set the MCPTT private emergency alert state to "MPEA 1: no-alert". and

ii) shall release the session as specified in the procedures of subclause 11.1.3.1.1.1 with the following clarifications:

A) shall include in the SIP BYE request an application/vnd.3gpp.mcptt-info+xml MIME body containing a <release-reason> element set to a value of "authentication of the MIKEY-SAKE I_MESSAGE failed"; and

B) shall skip the remaining steps in the present subclause; and

e) if the signature of the MIKEY-SAKKE I_MESSAGE was successfully validated:

i) shall extract and decrypt the encapsulated PCK using the originating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [78]; and

ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [46];

NOTE: With the PCK successfully shared between the originating MCPTT client and the terminating MCPTT client, both clients are able to use SRTP/SRTCP to create an end-to-end secure session;

3) if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested" or "MEPC 3: emergency-pc-granted", shall perform the actions specified in subclause 6.2.8.3.4; and

4) shall notify the user that the call has been successfully established.

On receiving a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request:

1) if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested"; or

2) if the MCPTT emergency private call state is set to "MEPC 3: emergency-pc-granted";

the MCPTT client shall perform the actions specified in subclause 6.2.8.3.5.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing session, the MCPTT client shall follow the actions specified in subclause 6.2.8.3.7.

11.1.1.2.1.2 Client terminating procedures

Upon receipt of an initial SIP INVITE request, the MCPTT client shall follow the procedures for termination of multimedia sessions in the IM CN subsystem as specified in 3GPP TS 24.229 [4] with the clarifications below.

The MCPTT client:

1) may reject the SIP INVITE request if any of the following conditions are met:

a) MCPTT client is already occupied in another session and the number of simultaneous sessions exceeds <MaxCall>, the maximum simultaneous MCPTT session for private call, as specified in TS 24.484 [50];

b) MCPTT client does not have enough resources to handle the call; or

c) any other reason outside the scope of this specification;

otherwise, continue with the rest of the steps.

NOTE 1: If the SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element set to a value of "true", the participating MCPTT function can choose to accept the request.

2) if the SIP INVITE request is rejected in step 1), shall respond toward participating MCPTT function either with appropriate reject code as specified in 3GPP TS 24.229 [4] and warning texts as specified in subclause 4.4.2 or with SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure according to <allow-failure-restriction> as specified in 3GPP TS 24.484 [50] and skip the rest of the steps of this subclause;

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

   a) should display to the MCPTT user an indication that this is a SIP INVITE request for an MCPTT emergency private call and:

      i) should display the MCPTT ID of the originator of the MCPTT emergency private call contained in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

      ii) if the <alert-ind> element is set to "true", should display to the MCPTT user an indication of the MCPTT emergency alert and associated information; and

   b) if the session was established with a <session-type> of "first-to-answer"; shall temporarily save the current value of the MCPTT emergency private priority (MEPP) state;

NOTE 2: The current value of the MCPTT emergency private priority (MEPP) state needs to be temporarily saved because the MCPTT client may not be the one selected to terminate the first to answer emergency private call. Hence, the MCPTT client needs to be able to restore the MCPTT emergency private priority (MEPP) state to the saved value.

   c) shall set the MCPTT emergency private priority state to "MEPP 2: in-progress" for this private call;

4) if the SDP offer of the SIP INVITE request contains an "a=key-mgmt" attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

   a) shall extract the MCPTT ID of the originating MCPTT from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78];

   b) shall convert the MCPTT ID to a UID as described in 3GPP TS 33.180 [78];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [78];

   d) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails, shall reject the SIP INVITE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and include warning text set to "136 authentication of the MIKEY-SAKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4; and

   e) if the signature of the MIKEY-SAKKE I_MESSAGE was successfully validated:

      i) shall extract and decrypt the encapsulated PCK using the terminating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [78]; and

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [78];

NOTE 3: With the PCK successfully shared between the originating MCPTT client and the terminating MCPTT client, both clients are able to use SRTP/SRTCP to create an end-to-end secure session.

5) if an end-to-end security context needs to be established and if the <session-type> in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request is set to "first-to-answer" then:

   a) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [78];

b) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [78];

c) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect private call communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [78];

d) shall encrypt the PCK to a UID associated to the MCPTT client using the MCPTT ID and KMS URI of the originator of the SIP INVITE request as determined by the procedures of subclause 6.2.8.3.9 and a time related parameter as described in 3GPP TS 33.180 [78];

e) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [78];

f) shall add the MCPTT ID of the MCPTT user to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]; and

NOTE 4: The initiator of the MIKEY-SAKKE I_MESSAGE is in this case the terminating client from the perspective of the call.

g) shall sign the MIKEY-SAKKE I_MESSAGE using the MCPTT user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [78];

6) may check if a Resource-Priority header field is included in the incoming SIP INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

7) may display to the MCPTT user the MCPTT ID of the inviting MCPTT user;

8) if the <session-type> in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request is set to "first-to-answer":

a) shall notify the user of the incoming call;

b) shall not forward the first-to-answer call;

c) if the MCPTT user is busy on another call, shall send a SIP 486 (Busy Here) to the SIP INVITE request according to 3GPP TS 24.229 [4] and not continue with any further steps in this subclause; and

d) if the MCPTT user does not answer the call within a time decided by the client implementation, the MCPTT client shall send a SIP 480 (Temporarily Unavailable) to the SIP INVITE request according to 3GPP TS 24.229 [4] and not continue with any further steps in this subclause;

NOTE 5: In the conditions below, as the SIP layer implements the actions for commencement mode, it is assumed that the Answer-Mode or Priv-Answer-Mode header fields are set correctly in line with the setting of the <session-type> in the application/vnd.3gpp.mcptt-info+xml MIME body of the incoming SIP INVITE request.

9) shall perform the automatic commencement procedures specified in subclause 6.2.3.1.1 if one of the following conditions are met:

a) SIP INVITE request contains an Answer-Mode header field with the value "Auto" and the MCPTT service setting at the invited MCPTT client for answering the call is set to automatic commencement mode;

b) SIP INVITE request contains an Answer-Mode header field with the value "Auto" and the MCPTT service setting at the invited MCPTT client for answering the call is set to manual commencement mode, yet the invited MCPTT client is willing to answer the call with automatic commencement mode; or

c) SIP INVITE request contains a Priv-Answer-Mode header field with the value of "Auto"; and

10) shall perform the manual commencement procedures specified in subclause 6.2.3.2.1 if either of the following conditions are met:

a) SIP INVITE request contains an Answer-Mode header field with the value "Manual" and the MCPTT service setting at the invited MCPTT client for answering the call is set to manual commencement mode;

b) SIP INVITE request contains an Answer-Mode header field with the value "Manual" and the MCPTT service setting at the invited MCPTT client for answering the call is set to automatic commencement mode, yet the invited MCPTT client allows the call to be answered with manual commencement mode; or

c) SIP INVITE request contains a Priv-Answer-Mode header field with the value of "Manual".

Upon receiving the SIP CANCEL request cancelling a SIP INVITE request for which a dialog exists at the MCPTT client and a SIP 200 (OK) response has not yet been sent to the SIP INVITE request then the MCPTT client:

1) if the session was established with a <session-type> of "first-to-answer", may notify the MCPTT user of the cancellation of the call;

2) if a temporary MCPTT emergency private priority (MEPP) state value was saved in step 3) b) above:

   a) shall restore the MCPTT emergency private priority (MEPP) state to the temporary MCPTT emergency private priority (MEPP) state value; and

   b) shall discard the temporary MCPTT emergency private priority (MEPP) state value;

3) shall send a SIP 200 (OK) response to the SIP CANCEL request according to 3GPP TS 24.229 [4]; and

4) shall send a SIP 487 (Request Terminated) response to the SIP INVITE request according to 3GPP TS 24.229 [4].

Upon receiving a SIP BYE request for an established dialog, the MCPTT client:

1) if the session was established with a <session-type> of "first-to-answer" and:

   a) if the received SIP BYE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <release-reason> element set to a value of "not selected for call" or "authentication of the MIKEY-SAKE I_MESSAGE failed":

      i) if a temporary MCPTT emergency private priority (MEPP) state value was saved in step 3) b) above, shall restore the MCPTT emergency private priority (MEPP) state to the the temporary MCPTT emergency private priority (MEPP) state value saved in step 3) b) above; and

   b) may notify the MCPTT user of the release of the call; and

2) shall follow the procedures in subclause 11.1.4.2.

NOTE 6: The above conditions for SIP CANCEL and SIP BYE cover the case for a first-to-answer call where the MCPTT server has already established the private call with another MCPTT client and needs to immediately cancel or release the dialogs with other MCPTT clients.

11.1.1.2.1.3 Client terminating procedures for reception of SIP re-INVITE request

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

Upon receipt of a SIP re-INVITE request for an existing private call session, the MCPTT client shall:

1) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "true":

   a) should display to the MCPTT user an indication that this is a SIP re-INVITE request to upgrade this call to an MCPTT emergency private call and:

      i) should display the MCPTT ID of the originator of the MCPTT emergency private call contained in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

      ii) if the <alert-ind> element is set to "true", should display to the MCPTT user an indication of the MCPTT emergency alert and associated information; and

   b) shall set the MCPTT emergency private priority state to "MEPP 2: in-progress" for this private call;

2) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind> element set to a value of "false":

   a) should display to the MCPTT user an indication that this is a SIP re-INVITE request to downgrade this emergency private call to a normal priority private call and:

      i) should display the MCPTT ID of the sender of the SIP re-INVITE request contained in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

      ii) if the <alert-ind> element is set to "false" should display to the MCPTT user an indication that the MCPTT emergency alert is cancelled;

      iii) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body including an <originated-by> element:

         A) should display to the MCPTT user the MCPTT ID contained in the <originated-by> element of the MCPTT user that originated the MCPTT emergency alert; and

         B) if the MCPTT ID contained in the <originated-by> element is the MCPTT ID of the receiving MCPTT user, shall set the MCPTT emergency alert state to "MPEA 1: no-alert";

   b) shall set the MCPTT emergency private priority state to "MEPP 1: no-emergency" for this private call; and

   c) if the MCPTT emergency private call state of the call is set to "MEPC 3: emergency-call-granted", shall set the MCPTT emergency private call state of the call to "MEPC 1: emergency-pc-capable";

3) may check if a Resource-Priority header field is included in the incoming SIP INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

4) may display to the MCPTT user the MCPTT ID of the inviting MCPTT user if not done so in step 1 or step 2 above;

NOTE 1: As this is a re-INVITE for an existing MCPTT private call session, there is no attempt made to change the answer-mode from its current state.

5) shall accept the SIP re-INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [4];

6) if the SIP re-INVITE request was received within an on-demand session, shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP INVITE request according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.2;

7) if the SIP re-INVITE request was received within a pre-established session, shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session;

NOTE 2: The SIP re-INVITE request can be received within an on-demand session or a pre-established session. If the SIP re-INVITE request is received within a pre-established session, the media-level section for the MCPTT speech media stream and the media-level section of the media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

8) shall send the SIP 200 (OK) response towards the MCPTT server according to rules and procedures of 3GPP TS 24.229 [4]; and

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

11.1.1.2.1.4 MCPTT in-progress emergency cancel

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

Upon receiving a request from an MCPTT user to cancel the in-progress emergency condition on an MCPTT emergency private call, the MCPTT client shall generate a SIP re-INVITE request by following the UE session procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) if the MCPTT user is not authorised to cancel the in-progress emergency condition on an MCPTT emergency private call as determined by the procedures of subclause 6.2.8.3.1.2, the MCPTT client:

   a) should indicate to the MCPTT user that they are not authorised to cancel the in-progress emergency condition on an MCPTT emergency private call; and

   b) shall skip the remaining steps of the current subclause;

2) shall, if the MCPTT user is cancelling an in-progress emergency condition and optionally an MCPTT emergency alert originated by the MCPTT user, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.3.6;

3) shall, if the MCPTT user is cancelling an in-progress emergency condition and optionally an MCPTT emergency alert originated by another MCPTT user, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.3.8;

4) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.3.3;

5) shall include in the SIP re-INVITE request an SDP offer the media parameters as currently established;

NOTE 1: The SIP re-INVITE request can be sent within an on-demand session or a pre-established session associated with an MCPTT group session. If the SIP re-INVITE request is sent within a pre-established session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

6) if an implicit floor request is required, shall indicate this as specified in subclause 6.4; and

7) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP re-INVITE request, the MCPTT client:

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

2) shall set the MCPTT emergency private priority state of the MCPTT private call to "MEPP 1: no-emergency";

3) shall set the MCPTT emergency private call state of the call to "MEPC 1: emergency-pc-capable"; and

4) if the MCPTT emergency alert state is set to "MPEA 4: Emergency-alert-cancel-pending", the sent SIP re-INVITE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body and the SIP 2xx response to the SIP request for a priority group call does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", shall set the MCPTT emergency alert state to "MPEA 1: no-alert".

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request:

1) if the SIP 4xx response, SIP 5xx response or SIP 6xx response contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <emergency-ind> element set to a value of "true", the MCPTT client shall set the MCPTT emergency private priority state as "MEPP 2: in-progress";

2) if the SIP 4xx response, SIP 5xx response or SIP 6xx response contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to a value of "true" and the sent SIP re-INVITE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, the MCPTT client shall set the MCPTT emergency alert state to "MPEA 3: emergency-alert-initiated"; and

3) if the SIP 4xx response, SIP 5xx response or SIP 6xx response did not contain an application/vnd.3gpp.mcptt-info+xml MIME body, shall set the MCPTT emergency private priority state as "MEPP 2: in-progress" and the MCPTT emergency alert (MPEA) state shall revert to its value prior to entering the current procedure.

NOTE 2: If the in-progress emergency private priority state cancel request is rejected, the state of the session does not change, i.e. continues with MCPTT emergency private call level priority.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.3.7.

11.1.1.2.1.5 Upgrade to MCPTT emergency private call

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

Upon receiving a request from an MCPTT user to upgrade the ongoing MCPTT private call to an MCPTT emergency private call, the MCPTT client shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [4], with the clarifications given below.

1) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in subclause 6.2.8.3.2;

2) shall include a Resource-Priority header field and comply with the procedures in subclause 6.2.8.3.3.

3) shall include an SDP offer with the media parameters as currently established according to 3GPP TS 24.229 [4];

NOTE: The SIP re-INVITE request can be sent within an on-demand session or a pre-established session associated with an MCPTT private call. If the SIP re-INVITE request is sent within a pre-established session, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

4) if an implicit floor request is required, shall indicate this as specified in subclause 6.4; and

5) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP re-INVITE request the MCPTT client:

1) shall interact with the user plane as specified in 3GPP TS 24.380 [5]; and

2) shall perform the actions specified in subclause 6.2.8.3.4.

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request, the MCPTT client shall perform the actions specified in subclause 6.2.8.3.5.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the MCPTT client shall follow the actions specified in subclause 6.2.8.3.7

11.1.1.2.2 Private call and first-to-answer call using pre-established session

11.1.1.2.2.1 Client originating procedures

Upon receiving a request from an MCPTT user to establish an MCPTT private call within a pre-established session the MCPTT client shall generate a SIP REFER request outside a dialog in accordance with the procedures specified in 3GPP TS 24.229 [4], IETF RFC 4488 [22] and IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27], with the clarifications given below.

If the MCPTT user is initiating a private call and an end-to-end security context needs to be established the MCPTT client:

1) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [78];

2) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [78];

3) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect private call communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [78];

4) shall encrypt the PCK to a UID associated to the MCPTT client using the MCPTT ID and KMS URI of the invited user as determined by the procedures of subclause 6.2.8.3.9 and a time related parameter as described in 3GPP TS 33.180 [78];

5) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [78];

6) shall add the MCPTT ID of the originating MCPTT to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]; and

7) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCPTT user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [78].

The MCPTT client populates the SIP REFER request as follows:

1) shall include the Request-URI set to the public service identity identifying the pre-established session on the MCPTT server serving the MCPTT user;

2) shall include the Refer-Sub header field with value "false" according to rules and procedures of IETF RFC 4488 [22];

3) shall include the Supported header field with value "norefersub" according to rules and procedures of IETF RFC 4488 [22];

4) shall include the option tag "multiple-refer" in the Require header field;

5) may include a P-Preferred-Identity header field in the SIP REFER request containing a public user identity as specified in 3GPP TS 24.229 [4];

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

7) shall set the Refer-To header field of the SIP REFER request as specified in IETF RFC 3515 [25] with a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [20], and with the Content-ID header field set to this "cid" URL.

8) for the initiation of a private call, shall include in the application/resource-lists MIME body a single <entry> element containing a "uri" attribute set to the MCPTT ID of the called user, extended with the following URI header fields:

NOTE 1: Characters that are not formatted as ASCII characters are escaped in the following URI header fields

   a) if force of automatic commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include a Priv-Answer-Mode header field with the value "Auto" according to the rules and procedures of IETF RFC 5373 [18];

   b) if force of automatic commencement mode at the invited MCPTT client is not requested by the MCPTT user and:

      i) if automatic commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include an Answer-Mode header field with the value "Automatic" according to rules and procedures of IETF RFC 5373 [18]; and

      ii) if manual commencement mode at the invited MCPTT client is requested by the MCPTT user, shall include an Answer-Mode header field with the value "Manual" according to rules and procedures of IETF RFC 5373 [18]; and

   c) shall include in a hname "body" URI header field:

      i) if the SDP parameters of the pre-established session do not contain a media-level section of a media-floor control entity or if end-to-end security is required for the private call, an application/sdp MIME body containing the SDP parameters of the pre-established session according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.1. If implicit floor control is required and the pre-established session was not established with an implicit floor request, then the application/sdp MIME body shall contain an implicit floor request as specified in subclause 6.4; and

      ii) an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element set to "private";

9) for an initiation of a first-to-answer call, shall include in the application/resource-lists MIME body an <entry> element for each of the targeted MCPTT users, with each <entry> element containing a "uri" attribute set to the MCPTT ID of the targeted user, extended with hname "body" URI header field containing:

NOTE 2: Characters that are not formatted as ASCII characters are escaped in the following URI header fields

a) if the SDP parameters of the pre-established session do not contain a media-level section of a media-floor control entity, an application/sdp MIME body containing the SDP parameters of the pre-established session according to 3GPP TS 24.229 [4] with the clarification given in subclause 6.2.1. If implicit floor control is required and the pre-established session was not established with an implicit floor request, then the application/sdp MIME body shall contain an implicit floor request as specified in subclause 6.4; and

b) an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element set to "first-to-answer";

10) if the MCPTT user has requested the origination of an MCPTT emergency private call or is originating an MCPTT private call and the MCPTT emergency state is already set, the MCPTT client:

a) if this is an authorised request for an MCPTT emergency private call as determined by the procedures of subclause 6.2.8.3.1.1, shall comply with the procedures in subclause 6.2.8.3.2; and

b) if this is an unauthorised request for an MCPTT emergency private call as determined in step a) above, should indicate to the MCPTT user that they are not authorised to initiate an MCPTT emergency private call;

11) if the MCPTT emergency private priority state for this call is set to "MEPP 2: in-progress", the MCPTT client shall comply with the procedures in subclause 6.2.8.3.3; and

12) shall include a Target-Dialog header field as specified in IETF RFC 4538 [23] identifying the pre-established session.

The MCPTT client shall send the SIP REFER request towards the MCPTT server according to 3GPP TS 24.229 [4].

Upon receiving a final SIP 2xx response to the SIP REFER request the MCPTT client shall interact with media plane as specified in 3GPP TS 24.380 [5].

On receiving a SIP 4xx response, SIP 5xx response or a SIP 6xx response to the SIP REFER request for an MCPTT emergency private call:

1) if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested", the MCPTT client shall perform the actions specified in subclause 6.2.8.3.5; and

2) shall skip the remaining steps.

Upon receipt of a SIP re-INVITE request within the pre-established session targeted by the sent SIP REFER request, the MCPTT client:

1) if the sent SIP REFER request was a request to originate a first-to-answer call:

a) if the received SIP re-INVITE request contains an SDP offer including an a=key-mgmt attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

i) shall extract the MCPTT ID of the sender of the SIP 200 (OK) response from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78];

ii) shall convert the MCPTT ID to a UID as described in 3GPP TS 33.180 [78];

iii) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [78];

iv) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails:

A) shall set the MCPTT emergency private call state to "MEPC 1: emergency-pc-capable";

B) if the MCPTT emergency private priority state of the private call is "MEPP 3: confirm-pending" shall set the MCPTT emergency private priority state of the private call to "MEPP 1: no-emergency";

C) if the sent SIP request for an MCPTT emergency private call contained an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to a value of "true", shall set the MCPTT private emergency alert state to "MPEA 1: no-alert"; and

D) shall release the session as specified in the procedures of subclause 11.1.3.1.2.1 with the following clarifications:

I) shall include in the SIP BYE request an application/vnd.3gpp.mcptt-info+xml MIME body containing a <release-reason> element set to a value of "authentication of the MIKEY-SAKE I_MESSAGE failed"; and

II) shall skip the remaining steps in the present subclause; and

vii) if the signature of the MIKEY-SAKKE I_MESSAGE was successfully validated:

A) shall extract and decrypt the encapsulated PCK using the originating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [78]; and

B) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [78];

NOTE 3: With the PCK successfully shared between the originating MCPTT client and the terminating MCPTT client, both clients are able to use SRTP/SRTCP to create an end-to-end secure session;

2) if the sent SIP REFER request was a request for an MCPTT emergency private call:

a) if the MCPTT emergency private call state is set to "MEPC 2: emergency-pc-requested" or "MEPC 3: emergency-pc-granted":

i) shall set the MCPTT emergency private priority state of the call to "MEPP 2: in-progress" if it was not already set;

ii) shall set the MCPTT emergency private call state to "MEPC 3: emergency-pc-granted"; and

iii) if the MCPTT private emergency alert state is set to "MPEA 2: emergency-alert-confirm-pending" and:

A) if the SIP re-INVITE request contains an <alert-ind> element set to a value of "true" or does not contain an <alert-ind> element, shall set the MCPTT private emergency alert state to " MPEA 3: emergency-alert-initiated "; or

B) if the SIP re-INVITE request contains an <alert-ind> element set to a value of "false", shall set the MCPTT private emergency alert state to "MPEA 1: no-alert ";

3) shall check if a Resource-Priority header field is included in the incoming SIP re-INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

4) shall accept the SIP re-INVITE request and generate a SIP 200 (OK) response according to rules and procedures of 3GPP TS 24.229 [4];

5) shall include an SDP answer in the SIP 200 (OK) response to the SDP offer in the incoming SIP re-INVITE request according to 3GPP TS 24.229 [4], based upon the parameters already negotiated for the pre-established session; and

6) shall send the SIP 200 (OK) response towards the participating MCPTT function according to rules and procedures of 3GPP TS 24.229 [4].

On call release by interaction with the media plane as specified in subclause 9.2.2 of 3GPP TS 24.380 [5] if the sent SIP REFER request was a request for an MCPTT emergency private call, the MCPTT client shall perform the procedures specified in subclause 6.2.8.1.18.

11.1.1.2.2.2 Client terminating procedures

The MCPTT client shall follow the procedures for termination of multimedia sessions as specified in subclause 11.1.1.2.1.2 with the following clarifications:

1) if the MCPTT client is targeted for a new MCPTT emergency private call, the MCPTT client receives a SIP INVITE with an application/vnd.3gpp.mcptt-info+xml MIME body with an <emergency-ind> set to a value of "true"; or

2) if the MCPTT client is targeted for a new normal priority MCPTT private call, the MCPTT client receives a SIP re-INVITE request rather than a SIP INVITE request.

11.1.1.3 Participating MCPTT function procedures

11.1.1.3.1 Originating procedures

11.1.1.3.1.1 On-demand private call and first-to-answer call

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 "private" or "first-to-answer", the participating MCPTT function:

1) may reject the SIP INVITE request depending on the value of the Resource-Priority header field if the Resource-Priority header field is included in the received SIP INVITE request according to rules and procedures specified in IETF RFC 4412 [29] and shall not continue with the rest of the steps;

2) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the "SIP INVITE request for originating participating MCPTT function" 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 1: If the received SIP INVITE request contains an emergency indication set to a value of "true", the participating MCPTT function can choose to accept the request.

NOTE 2: If the received SIP INVITE request contains an emergency indication set to a value of "true", the participating MCPTT function can choose to allow an exception to the limit on the number of private calls and accept the request.

3) 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 user;

NOTE 3: 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.

4) if the participating MCPTT function cannot find a binding between the public user identity and an MCPTT ID or if the validity period of an existing binding has expired, then the participating MCPTT function shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

5) shall:

   a) if the <session-type> is set to "private", determine that the call is a private call; and

   b) if the <session-type> is set to "first-to-answer", determine that the call is a first-to-answer-call;

6) if the call is a:

   a) private call, determine the public service identity of the controlling MCPTT function for the private call service associated with the originating user's MCPTT ID identity; or

   b) first-to-answer, determine the public service identity of the controlling MCPTT function for the first-to-answer call service associated with the originating user's MCPTT ID identity;

7) if the participating MCPTT function is unable to identify the controlling MCPTT function for the private call service or first-to-answer call service associated with the originating user's MCPTT ID identity, it shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

8) if the incoming SIP INVITE request does not contain an application/resource-lists MIME body, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

9) if the call is a private call and the incoming SIP INVITE request contains an application/resource-lists MIME body with more than one <entry> element, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

10) if the <allow-private-call> element of the <ruleset> element is not present in the MCPTT user profile document on the participating MCPTT function or is present with the value "false" (see the MCPTT user profile document in 3GPP TS 24.484 [50]), indicating that the user identified by the MCPTT ID is not authorised to initiate private calls, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response, with warning text set to "107 user not authorised to make private calls" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

11) if the call is a private call and:

   a) if the received SIP INVITE request includes an Answer-Mode header field as specified in IETF RFC 5373 [18] with the value "Auto" and the <allow-automatic-commencement> element of the <ruleset> element is not present in the MCPTT user profile document on the participating MCPTT function or is present with the value "false" (see the MCPTT user profile document in 3GPP TS 24.484 [50]) indicating that the user identified by the MCPTT ID is not authorised to initiate private call with automatic commencement, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "125 user not authorised to make private call with automatic commencement" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

   b) if the received SIP INVITE request includes an Answer-Mode header field as specified in IETF RFC 5373 [18] with the value "Manual" and the <allow-manual-commencement> element of the <ruleset> element is not present in the MCPTT user profile document on the participating MCPTT function or is present with the value "false" (see the MCPTT user profile document in 3GPP TS 24.484 [50]), indicating that the user identified by the MCPTT ID is not authorised to initiate private call with manual commencement, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "126 user not authorised to make private call with manual commencement" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

   c) if the <PrivateCall> element exists in the MCPTT user profile document with one more <entry> elements (see the MCPTT user profile document in 3GPP TS 24.484 [50]) and:

      i) if the "uri" attribute of the <entry> element of the application/resource-lists MIME body does not match with one of the <entry> elements of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]); and

      ii) if configuration is not set in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) that allows the MCPTT user to make a private call to users not contained within the <entry> elements of the <PrivateCall> element;

   then:

      i) shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "144 user not authorised to call this particular user" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

12) if the call is a first-to-answer call and if the <PrivateCall> element exists in the MCPTT user profile document with one or more <entry> elements (see the MCPTT user profile document in 3GPP TS 24.484 [50]) and:

   a) if:

      i) the "uri" attribute of each and every <entry> element of the application/resource-lists MIME body does not match with any of the <entry> elements of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]); and

      ii) if configuration is not set in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) that allows the MCPTT user to make a private call to users not contained within the <entry> elements of the <PrivateCall> element;

then:

i) shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "153 user not authorised to call any of the users requested in the first-to-answer call" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

13) if the call is a first-to-answer call and:

a) if the <allow-request-first-to-answer-call> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false", (see the MCPTT user profile document in 3GPP TS 24.484 [50]);

then:

a) shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "156 user not authorised to originate a first-to-answer call" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

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

15) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.3 with the following clarifications:

a) if the conditions in step 12) above were executed and the participating MCPTT function determined that the "uri" attribute of only one of the <entry> elements of the application/resource-lists MIME body matched with an <entry> element of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) then the <session-type> in the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request generated in subclause 6.3.2.1.3 is set to "private"; and

b) if the conditions in step 12) above were executed, then only the <entry> element(s) of the application/resource-lists MIME body that have a "uri" attribute that matched with an <entry> elements of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) are included in the application/resource-lists MIME body in the SIP INVITE request generated in subclause 6.3.2.1.3;

16) shall set the Request-URI to the public service identity of the controlling MCPTT function hosting the private call service or first-to-answer call service as determined by step 6);

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

18) if the call is a private call and:

a) if a Priv-Answer-Mode header field specified in IETF RFC 5373 [18] was received in the incoming SIP INVITE request with a value of "Manual", shall not include a Priv-Answer-Mode header field in the outgoing SIP INVITE request;

b) if the <allow-force-auto-answer> element of the <ruleset> element is not present in the MCPTT user profile document on the participating MCPTT function or is present with the value "false" (see the MCPTT user profile document in 3GPP TS 24.484 [50]), and the Priv-Answer-Mode header field specified in IETF RFC 5373 [18] was received in the incoming SIP INVITE request with a value of "Auto", shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "143 not authorised to force auto answer" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

c) if the <allow-force-auto-answer> element of the <ruleset> element is present in the MCPTT user profile document with the value "true" (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the participating MCPTT function, and the Priv-Answer-Mode header field specified in IETF RFC 5373 [18] was received in the incoming SIP INVITE request with a value of "Auto", shall include the Priv-Answer-Mode header field set to a value of "Auto" in the outgoing SIP INVITE request;

d) if a Priv-Answer-Mode header field containing the value of "Auto" has not been included in the outgoing SIP INVITE request as specified in step 17) above and the incoming "SIP INVITE request for originating

participating MCPTT function" contained an Answer-Mode header field as specified in IETF RFC 5373 [18], then shall populate the Answer-Mode header field of the outgoing SIP INVITE request with the contents of the Answer-Mode header field from the incoming "SIP INVITE request for originating participating MCPTT function";

19) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received "SIP INVITE request for originating participating MCPTT function", as specified in subclause 6.3.2.1.1.1;

20) 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 if included in the SIP INVITE request from the MCPTT client; and

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

Upon receiving a SIP 180 (Ringing) response, the participating MCPTT function:

1) shall generate a SIP 180 (Ringing) response to the SIP INVITE request as specified in the subclause 6.3.2.1.5.1;

2) shall include the P-Asserted-Identity header field as received in the incoming SIP 180 (Ringing) response;

3) shall include Warning header field(s) received in the incoming SIP 180 (Ringing) response; and

4) shall forward the SIP 180 (Ringing) response to the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response, the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as specified in the subclause 6.3.2.1.5.2;

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

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

4) shall include the P-Asserted-Identity header field received in the incoming SIP 200 (OK) response into the outgoing SIP 200 (OK) response;

5) 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;

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

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

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

The participating MCPTT function shall forward any other SIP response that does not contain SDP, including any MIME bodies contained therein, along the signalling path to the originating network according to 3GPP TS 24.229 [4].

11.1.1.3.1.2 Private call and first-to-answer call initiation using pre-established session

Upon receipt of a "SIP REFER request for a pre-established session", with:

1) the Refer-To header field containing a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [20] containing one or more <entry> element(s) with a "uri" attribute containing a SIP-URI set to the MCPTT ID of the called user(s);

2) a body" URI header field of the SIP-URI specified above containing an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element set to "private" or "first-to-answer"; and

3) a Content-ID header field set to the "cid" URL;

the participating 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 1: If the application/vnd.3gpp.mcptt-info MIME body included in the SIP REFER request as described at the top of the present subclause contains an <emergency-ind> element or <imminentperil-ind> element 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 REFER request;

3) if the participating MCPTT function cannot find a binding between the public user identity and an MCPTT ID or if the validity period of an existing binding has expired, then the participating MCPTT function shall reject the SIP REFER request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

4) if the received SIP REFER request does not contain an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

5) if the received SIP REFER request contains an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field with more than one <entry> element each with an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element:

   a) not set to "first-to-answer", shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps; or

   b) set to "first-to-answer", determine that the call is a first-to-answer call;

6) if the received SIP REFER request contains an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field with only one <entry> element with an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element:

   a) not set to "private", shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps; or

   b) set to "private", determine that the call is a private call;

7) if the call is a:

   a) private call, shall determine the public service identity of the controlling MCPTT function for the private call service associated with the originating user's MCPTT ID; or

   b) first-to-answer call, shall determine the public service identity of the controlling MCPTT function for the first-to-answer call service associated with the originating user's MCPTT ID;

NOTE 2: How the participating MCPTT server discovers the public service identity of the controlling MCPTT function associated with the private call service or first-to-answer service of the calling user is out of scope of the current document.

8) if the participating MCPTT function is unable to identify the controlling MCPTT function for the private call service or first-to-answer call service associated with the originating user's MCPTT ID, it shall reject the REFER request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

9) if the <allow-private-call> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the participating MCPTT function or is present with the value "false", indicating that the user identified by the MCPTT ID is not authorised to initiate private calls, shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response to the SIP INVITE request, with warning text set to "107 user not authorised to make private calls" in a Warning header field as specified in subclause 4.4;

10) if the call is a private call:

a) if the received SIP REFER request includes an Answer-Mode header field as specified in IETF RFC 5373 [18] set to "Auto" contained in the header portion of the SIP URI present in the application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, and the <allow-automatic-commencement> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the participating MCPTT function or is present with the value "false" (indicating that the user identified by the MCPTT ID is not authorised to initiate private call with automatic commencement), shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response including warning text set to "125 user not authorised to make private call with automatic commencement" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

b) if the received SIP REFER request includes an Answer-Mode header field as specified in IETF RFC 5373 [18] set to "Manual" contained in the header portion of the SIP URI present in the application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, and the <allow-manual-commencement> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the participating MCPTT function or is present with the value "false" (indicating that the user identified by the MCPTT ID is not authorised to initiate private call with manual commencement), shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response including warning text set to "126 user not authorised to make private call with manual commencement" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

c) if the <allow-force-auto-answer> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the participating MCPTT function or is present with the value "false", and the SIP REFER request contained a Priv-Answer-Mode header field as specified in IETF RFC 5373 [18] set to "Auto" in the header portion of the SIP URI in the application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "143 not authorised to force auto answer" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

d) if the <PrivateCall> element exists in the MCPTT user profile document with one more <entry> elements (see the MCPTT user profile document in 3GPP TS 24.484 [50]) and:

i) if the SIP-URI in the application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field not match with one of the <entry> elements of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]); and

ii) if configuration is not set in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) that allows the MCPTT user to make a private call to users not contained within the <entry> elements of the <PrivateCall> element;

then:

i) shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "144 user not authorised to call this particular user" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

11) if the call is a first-to-answer call and if the <PrivateCall> element exists in the MCPTT user profile document with one or more <entry> elements (see the MCPTT user profile document in 3GPP TS 24.484 [50]) and:

a) the "uri" attribute of each and every <entry> element of the application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field does not match with any of the <entry> elements of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]); and

b) if configuration is not set in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) that allows the MCPTT user to make a private call to users not contained within the <entry> elements of the <PrivateCall> element;

then:

a) shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "153 user not authorised to call any of the users requested in the first-to-answer call" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

12) if the call is a first-to-answer call and:

a) if the <allow-request-first-to-answer-call> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false", (see the MCPTT user profile document in 3GPP TS 24.484 [50]);

then:

a) shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "156 user not authorised to originate a first-to-answer call" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

13) if the "SIP REFER request for a pre-established session" contained a Refer-Sub header field containing "false" value and a Supported header field containing "norefersub" value, shall handle the SIP REFER request as specified in 3GPP TS 24.229 [4], IETF RFC 3515 [25] as updated by IETF RFC 6665 [26], and IETF RFC 4488 [22] without establishing an implicit subscription;

14) shall generate a final SIP 200 (OK) response to the "SIP REFER request for a pre-established session" according to 3GPP TS 24.229 [4];

NOTE 3: In accordance with IETF RFC 4488 [22], the participating MCPTT function inserts the Refer-Sub header field containing the value "false" in the SIP 200 (OK) response to the SIP REFER request to indicate that it has not created an implicit subscription.

15) shall send the response to the "SIP REFER request for a pre-established session" towards the MCPTT client according to 3GPP TS 24.229 [4];

16) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.4 with the following clarifications:

a) if the conditions in step 11) above were executed and the participating MCPTT function determined that the "uri" attribute of only one of the <entry> elements of the application/resource-lists MIME body matched with an <entry> element of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) then the <session-type> in the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request generated in subclause 6.3.2.1.4 is set to "private"; and

b) if the conditions in step 11) above were executed, then only the <entry> element(s) of the application/resource-lists MIME body that have a "uri" attribute that matched with an <entry> elements of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) are included in the application/resource-lists MIME body in the SIP INVITE request generated in subclause 6.3.2.1.3;

17) shall set the Request-URI of the SIP INVITE request to the public service identity of the controlling MCPTT function hosting the private call service or first-to-answer call service for the calling MCPTT user as determined above in step 7);

18) if the call is a private call:

a) if the SIP REFER request contained a Priv-Answer-Mode header field as specified in IETF RFC 5373 [18] set to "Manual" in the header portion of the SIP URI in the application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, shall copy the Priv-Answer-Mode header field from the incoming SIP REFER request to the outgoing SIP INVITE request;

b) if the <allow-force-auto-answer> element of the <ruleset> element is present in the MCPTT user profile document with the value "true" (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the participating MCPTT function, and the Priv-Answer-Mode header field specified in IETF RFC 5373 [18] was received in the header portion of the SIP URI in the application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, with a value set to "Auto", shall copy the Priv-Answer-Mode header field to the outgoing SIP INVITE request; and

c) if a Priv-Answer-Mode header field containing the value of "Auto" has not been copied to the outgoing SIP INVITE request as specified in step 16) above, and the incoming SIP REFER request contained an Answer-Mode header field in the headers portion of the SIP URI in the application/resource-lists referenced by a "cid" URL in the Refer-To header field, then copy the Answer-Mode header field to the outgoing SIP INVITE request;

19) if the received SIP REFER request contained a Resource-Priority header field, shall include in the outgoing SIP INVITE request 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 received SIP REFER request; and

NOTE 4: The participating MCPTT function will leave verification of the Resource-Priority header field to the controlling MCPTT function.

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

Upon receiving SIP provisional responses for the SIP INVITE request the participating MCPTT function:

1) shall discard the received SIP responses without forwarding them.

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

1) if:

a) the received SIP 2xx response was in response to a request for an MCPTT private call; or

b) the received SIP 2xx response was in response to a SIP INVITE request for a first-to-answer call which did not include an a=key-mgmt "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE in the SDP answer;

then:

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

2) if the received SIP 2xx response was in response to a request for an MCPTT emergency private call and does not contain a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149":

a) shall generate a SIP re-INVITE request to be sent towards the MCPTT client within the pre-established session as specified in subclause 6.3.2.1.8.6;

b) shall send the SIP re-INVITE request towards the MCPTT client within the pre-established session according to 3GPP TS 24.229 [4]; and

c) if the received SIP 2xx response was in response to a request for a first-to-answer call, upon receipt of a SIP 2xx response to the SIP re-INVITE, shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

3) if the received SIP 2xx response was in response to a SIP INVITE request for a first-to-answer call which was not a request for an MCPTT emergency private call and contains an SDP answer including an a=key-mgmt "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE, the participating MCPTT function:

a) shall generate a SIP re-INVITE request as specified in subclause 6.3.2.1.8.7;

b) shall send the SIP re-INVITE request towards the originating MCPTT client according to 3GPP TS 24.229 [4]; and

c) upon receipt of a SIP 2xx response to the SIP re-INVITE, shall interact with the media plane as specified in 3GPP TS 24.380 [5].

Upon receiving a SIP INFO request from the controlling MCPTT function within the dialog of the SIP INVITE request for an MCPTT emergency private call, the participating MCPTT function shall:

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

2) shall generate a SIP re-INVITE request to be sent towards the MCPTT client within the pre-established session as specified in subclause 6.3.2.1.8.6; and

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

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request in step 20) the participating MCPTT function:

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

11.1.1.3.1.3 Receipt of SIP re-INVITE for MCPTT private call from the served user

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

Upon receipt of a SIP re-INVITE request for an existing MCPTT private call session the participating MCPTT function:

1) may reject the SIP re-INVITE request depending on the value of the Resource-Priority header field if the Resource-Priority header field is included in the received SIP re-INVITE request according to rules and procedures specified in IETF RFC 4412 [29] and skip the rest of the steps;

2) if unable to process the request due to a lack of resources or a risk of congestion exists, may reject the "SIP INVITE request for originating participating MCPTT function" 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];

NOTE 1: If the SIP re-INVITE request contains an emergency indication, the participating MCPTT function can choose to accept the request.

3) 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 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.

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

NOTE 3: If the received SIP re-INVITE request is received within a pre-established session, associated with an MCPTT private call, the media-level section for the offered MCPTT speech media stream and the media-level section of the offered media-floor control entity are expected to be the same as was negotiated in the existing pre-established session.

5) shall generate a SIP re-INVITE request as specified in subclause 6.3.2.1.9;

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

7) shall, if the SIP re-INVITE request was received within an on-demand session include in the SIP re-INVITE request an SDP containing the current media parameters used by the existing session;

8) shall, if the SIP re-INVITE request was received within a pre-established session, include in the SIP re-INVITE request an SDP offer based upon the previously negotiated SDP for the pre-established session as specified in subclause 6.3.2.1.1.2;

9) 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 if included in the SIP re-INVITE request from the MCPTT client; and

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

Upon receiving a SIP 200 (OK) response, the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as specified in the subclause 6.3.2.1.5.2;

2) if the SIP 200 (OK) response is to be sent within an on-demand session shall include in the SIP 200 (OK) response an SDP answer as specified in the subclause 6.3.2.1.2.1;

3) if the SIP 200 (OK) response is to be sent within a pre-established session shall include in the SIP 200 (OK) response an SDP answer based upon the previously negotiated SDP for the pre-established session;

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

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

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

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

The participating MCPTT function shall forward any other SIP response that does not contain SDP, including any MIME bodies contained therein, along the signalling path to the originating network according to 3GPP TS 24.229 [4].

11.1.1.3.2 Terminating procedures

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

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 for terminating participating MCPTT function" 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 received SIP INVITE request contains an emergency indication set to a value of "true", the participating MCPTT function can 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 <session-type> element of the application/vnd.3gpp.mcptt-info+xml MIME body is set to "private" and 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) when the called user identified by the MCPTT ID is unable to participate in private calls as identified in the called user's MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the terminating participating MCPTT function, shall reject the "SIP INVITE request for terminating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "127 user not authorised to be called in private call" in a Warning header field as specified in subclause 4.4;

7) shall perform the automatic commencement procedures specified in subclause 6.3.2.2.5.1 and according to IETF RFC 5373 [18] if one of the following conditions are met:

   a) "SIP INVITE request for terminating participating MCPTT function" contains an Answer-Mode header field with the value "Auto";

   b) "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"; or

c) "SIP INVITE request for terminating participating MCPTT function" contains a Priv-Answer-Mode header field with the value "Auto"; 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 either of the following conditions are met:

a) "SIP INVITE request for terminating participating MCPTT function" contains an Answer-Mode header field with the value "Manual";

b) "SIP INVITE request for terminating participating MCPTT function" does not contain an Answer-Mode header field and 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"; or

c) "SIP INVITE request for terminating participating MCPTT function" contains a Priv-Answer-Mode header field with the value "Manual".

11.1.1.3.3 Receipt of SIP re-INVITE request by terminating participating function

This subclause covers the on-demand session case only.

Upon receipt of a SIP re-INVITE request for an existing MCPTT private call session 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 re-INVITE 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 skip the rest of the steps;

NOTE 1: If the SIP re-INVITE request contains an emergency indication, the participating MCPTT function can choose to accept the request.

2) 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 re-INVITE request to retrieve the binding between the MCPTT ID and public user identity;

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

4) shall generate a SIP re-INVITE as specified in subclause 6.3.2.2.10;

NOTE 2: As this is the modification of an in-progress MCPTT private call, this procedure does not attempt modification of the existing answer-mode of the call.

5) shall include in the SIP re-INVITE request an SDP offer containing the current media parameters used by the existing session; and

6) shall send the SIP re-INVITE request towards the MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving the SIP 200 (OK) response to the SIP re-INVITE request, the participating MCPTT function:

1) shall generate a SIP 200 (OK) response as described in the subclause 6.3.2.2.4.2;

2) shall include in the SIP 200 (OK) response an SDP answer based on the SDP answer in the received SIP 200 (OK) response as specified in subclause 6.3.2.2.2.1;

3) shall copy the P-Asserted-Identity header field from the incoming SIP 200 (OK) response to the outgoing SIP 200 (OK) response;

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

5) shall forward the SIP 200 (OK) response according to 3GPP TS 24.229 [4].

The participating MCPTT function shall forward any other SIP response that does not contain SDP along the signalling path to the originating network according to 3GPP TS 24.229 [4].

11.1.1.4 Controlling MCPTT function procedures

11.1.1.4.1 Originating procedures

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 11.1.1.4.2

The controlling MCPTT function:

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

NOTE 1: As a result of calling subclause 6.3.3.1.2, the <mcptt-calling-user-id> containing the calling user's MCPTT ID is copied into the outgoing SIP INVITE.

2) if the received SIP INVITE request contains an authorised request for an MCPTT emergency private call as determined by subclause 6.3.3.1.13.2:

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

   b) if the received SIP INVITE request contains an alert indication set to a value of "true" and this is an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, perform the procedures specified in subclause 6.3.3.1.12; and

   c) if the received SIP INVITE request did not contain an alert indication or contains an alert indication set to a value of "true" and is not an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, shall set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false";

3) if the received SIP INVITE request contained a <session-type> element in an application/vnd.3gpp.mcptt-info+xml MIME body set to "first-to-answer" shall include in the SIP INVITE request a Priv-Answer-Mode header field with the value "Manual" according to the rules and procedures of IETF RFC 5373 [18];

4) shall copy the MCPTT ID of the MCPTT user listed in the MIME resources body of the incoming SIP INVITE request, into the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the outgoing SIP INVITE request;

5) 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 2: How the controlling MCPTT function finds the address of the terminating MCPTT participating function is out of the scope of the current release.

NOTE 3: 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.

6) shall copy the public user identity of the calling MCPTT user from the P-Asserted-Identity header field of the incoming SIP INVITE request into the P-Asserted-Identity header field of the SIP INVITE request;

7) shall include a Resource-Priority header field populated with the values for an MCPTT emergency private call as specified in subclause 6.3.3.1.19, if either of the following conditions is met:

   a) if the received SIP INVITE request contains an authorised request for an MCPTT emergency private call as determined in step 2 above; or

   b) the originating MCPTT user is in an in-progress emergency private call state with the targeted MCPTT user;

8) 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;

9) shall send the SIP INVITE request towards the core network according to 3GPP TS 24.229 [4]; and

10) shall start a private call timer with a value set to the configured max private call duration for the user.

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

1) shall cache the contact received in the Contact header field; and

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

Upon expiry of the private call timer, the controlling MCPTT function shall follow the procedure for releasing private call session as specified in subclause 11.1.4.4.

11.1.1.4.2 Terminating procedures

In the procedures in this subclause:

1) <emergency–ind> refers to the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body;

2) <alert–ind> refers to the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

3) <session-type> refers to the <session-type> element of an application/vnd.3gpp.mcptt-info+xml MIME body.

Upon receipt of:

- a "SIP INVITE request for controlling MCPTT function of a private call"; or

- a "SIP INVITE request for controlling MCPTT function of a first-to-answer call";

the controlling MCPTT function:

1) if the <session-type> in the SIP INVITE request is set to "private":

   a) shall check whether the public service identity contained in the Request-URI is allocated for private call and perform the actions specified in subclause 6.3.7.1 if it is not allocated and skip the rest of the steps; and

   b) shall perform actions to verify the MCPTT ID of the inviting MCPTT user in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request, and authorise the request according to local policy, and if it is not authorised the controlling MCPTT function shall return a SIP 403 (Forbidden) response with the warning text as specified in "Warning header field" and skip the rest of the steps;

2) if the <session-type> in the SIP INVITE request is set to "first-to-answer" shall check whether the public service identity contained in the Request-URI is allocated for first-to-answer call and perform the actions specified in subclause 6.3.7.1 if it is not allocated and skip the rest of the steps;

3) if the incoming SIP INVITE request does not contain an application/resource-lists MIME body shall reject the SIP INVITE request with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

4) if the <session-type> is set to "private" and the application/resource-lists MIME body contains more than one <entry> element, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

5) shall validate that the received SDP offer includes at least one media stream for which the media parameters and at least one codec or media format is acceptable by the controlling MCPTT function and if not, reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

6) if received SIP INVITE request includes an <emergency-ind>, shall validate the request as described in subclause 6.3.3.1.17;

7) if the received SIP INVITE request contains an unauthorised request for an MCPTT emergency private call as determined by subclause 6.3.3.1.13.2:

   a) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response as specified in subclause 6.3.3.1.14; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

8) if a Resource-Priority header field is included in the received SIP INVITE request and if the Resource-Priority header field is set to the value indicated for emergency calls, shall reject the SIP INVITE request with a SIP 403 (Forbidden) response and skip the remaining steps if neither one of the following conditions are true:

   a) the SIP INVITE request does not contain an authorised request for an MCPTT emergency call as determined in step 4 above; or

   b) the originating MCPTT user is not in an in-progress emergency private call state with the targeted MCPTT user;

9) if:

   a) the received SIP INVITE request contains an emergency indication set to a value of "true";

   b) the originating MCPTT user is not in an in-progress emergency private call state with the targeted MCPTT user; and

   c) if the <session-type> in the SIP INVITE request is set to "private";

   then:

   a) shall cache the information that the MCPTT user has initiated an MCPTT emergency private call to the targeted user; and

   b) shall cache the information that the MCPTT user is in an in-progress emergency private call state with the targeted MCPTT user;

10) shall perform actions as described in subclause 6.3.3.2.2;

11) shall allocate an MCPTT session identity for the MCPTT session; and

12) shall invite the MCPTT user(s) listed in the MIME resource-lists body of received SIP INVITE request as specified in subclause 11.1.1.4.1.

Upon receiving a SIP 180 (Ringing) response and if the SIP 180 (Ringing) response or the SIP final response has not yet been sent to the inviting MCPTT client, the controlling MCPTT function:

1) if the SIP 180 (Ringing) response is associated with a SIP INVITE that contained a <session-type> set to "private", shall generate a SIP 180 (Ringing) response to the SIP INVITE request and send the SIP 180 (Ringing) response towards the inviting MCPTT client according to 3GPP TS 24.229 [4]; and

2) if the SIP 180 (Ringing) response is associated with a SIP INVITE that contained a <session-type> set to "first-to-answer", and no other SIP 180 (Ringing) responses have been received that are associated with a SIP INVITE that contained a <session-type> set to "first-to-answer", shall generate a SIP 183 (Session Progress) response to the SIP INVITE request and send the SIP 183 (Session Progress) response towards the inviting MCPTT client according to 3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request, the SIP dialog was established as a result of receiving a SIP INVITE request with a <session-type> element set to the value of "private" and the SIP final response has not yet been sent to the inviting MCPTT client, the controlling MCPTT function:

1) shall generate a SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.3.2.3.2 before continuing with the rest of the steps;

2) 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 6.3.3.2.2;

3) if the received SIP INVITE request contains an alert indication set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

NOTE 1: This is the case when the MCPTT user's request for an MCPTT emergency private call was granted but the request for the MCPTT emergency alert was denied.

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

NOTE 2: Resulting media plane processing is completed before the next step is performed.

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

Upon receiving a SIP 200 (OK) response for the SIP INVITE request, the SIP dialog was established as a result of receiving a SIP INVITE request with a <session-type> element set to the value of "first-to-answer" and the SIP final response has not yet been sent to the inviting MCPTT client the controlling MCPTT function:

1) shall generate a SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.3.2.3.2 before continuing with the rest of the steps;

2) 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;

3) the received SIP INVITE request contains an emergency indication set to a value of "true":

   a) shall cache the information that the MCPTT user has initiated an MCPTT emergency private call to the targeted user; and

   b) shall cache the information that the MCPTT user is in an in-progress emergency private call state with the targeted MCPTT user;

4) if the received SIP INVITE request contains an alert indication set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4;

NOTE 3: This is the case when the MCPTT user's request for an MCPTT emergency private call was granted but the request for the MCPTT emergency alert was denied.

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

NOTE 4: Resulting media plane processing is completed before the next step is performed.

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

7) for all other MCPTT clients that were invited due to the controlling MCPTT function receiving a SIP INVITE request with a <session-type> element set to the value of "first-to-answer":

   a) shall send a SIP BYE request to release a SIP dialog that has been established since the SIP 200 (OK) response was sent in step 5) by following the procedures in subclause 6.3.3.1.5 with the clarification that the SIP BYE request contain an application/vnd.3gpp.mcptt-info+xml MIME body including a <release-reason> element set to a value of "not selected for call";

   b) shall generate and send a SIP CANCEL request according SIP IETF RFC 3261 [24], to cancel a SIP dialog that has not yet been established since the SIP 200 (OK) response was sent in step 5);

   c) on receiving a SIP 200 (OK) to a SIP CANCEL request, shall wait to receive a SIP 487 (Request Terminated) to the original SIP INVITE request sent to the client; and

   d) if a SIP 487 (Request Terminated) from the MCPTT client is not received within a time determined by the MCPTT server implementation, shall send a SIP BYE towards the MCPTT client by following the procedures in subclause 6.3.3.1.5 with the clarification that the SIP BYE request contain an application/vnd.3gpp.mcptt-info+xml MIME body including a <release-reason> element set to a value of "not selected for call"; and

8) if not successful in cancelling or terminating SIP dialogs in step 6) above, may repeat the SIP CANCEL and SIP BYE requests.

Upon receiving a SIP ACK to the SIP 200 (OK) response sent towards the inviting MCPTT client, where the SIP 200 (OK) response was sent with a Warning header field as specified in subclause 4.4 with the warning text containing the mcptt-warn-code set to "149", the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.18.

The controlling MCPTT function shall forward any other SIP response that does not contain SDP, including any MIME bodies contained therein, along the signalling path to the originating network according to 3GPP TS 24.229 [4].

Upon receiving a SIP BYE request from the originating MCPTT client containing an application/vnd.3gpp.mcptt-info+xml MIME body containing a <release-reason> element set to a value of "authentication of the MIKEY-SAKE I_MESSAGE failed", the controlling MCPTT function:

1) if the received "SIP INVITE request for controlling MCPTT function of a first-to-answer call" contains an emergency indication set to a value of "true":

   a) shall delete from cache the information that the MCPTT user has initiated an MCPTT emergency private call to the targeted user; and

b) shall delete from cache the information that the MCPTT user is in an in-progress emergency private call state with the targeted MCPTT user; and2) shall follow the procedures in subclause 11.1.3.3.1.

11.1.1.4.3 Receiving a SIP re-INVITE for upgrade to emergency private call

In the procedures in this subclause:

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

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

Upon receiving a SIP re-INVITE request with an emergency indication set to a value of "true", the controlling MCPTT function:

1) shall validate that the received SDP offer includes at least one media stream for which the media parameters and at least one codec or media format is acceptable by the controlling MCPTT function and if not, reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

2) shall validate the request as described in subclause 6.3.3.1.17;

3) if the SIP re-INVITE request contains an unauthorised request for an MCPTT emergency private call as determined by subclause 6.3.3.1.13.2:

   a) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response as specified in subclause 6.3.3.1.14; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

4) if a Resource-Priority header field is included in the received SIP re-INVITE request and if the Resource-Priority header field is set to the value indicated for emergency calls, shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response and skip the remaining steps if neither of the following conditions are true:

   a) the SIP re-INVITE request does contains an authorised request for an MCPTT emergency call as determined in step 2 above; or

   b) the originating MCPTT user is in an in-progress emergency private call state with the targeted MCPTT user;

5) if the SIP re-INVITE request contains an emergency indication set to a value of "true" and the originating MCPTT user is not in an in-progress emergency private call state with the targeted MCPTT user:

   a) shall cache the information that the MCPTT user is in an in-progress emergency private call state with the targeted MCPTT user; and

   b) if the SIP re-INVITE request contains an alert indication set to "true" and this is an authorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall cache the information that the MCPTT user has sent an MCPTT emergency alert to the targeted user; and

6) shall send a SIP re-INVITE invite towards the MCPTT user listed in the MIME resource-lists body of received SIP re-INVITE request as specified in subclause 11.1.1.4.5.

Upon receiving a SIP 200 (OK) response for the SIP re-INVITE request and if the SIP response has not yet been sent to the inviting MCPTT client, the controlling MCPTT function:

1) shall generate a SIP 200 (OK) response to the SIP re-INVITE request as specified in the subclause 6.3.3.2.3 before continuing with the rest of the steps;

2) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP re-INVITE request containing the current media parameters used by the existing session;

3) if the received SIP re-INVITE request contains an alert indication set to a value of "true" and this is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4.

NOTE: When a SIP 200 (OK) response sent to the originator as a response to a SIP INVITE request that contained authorised request(s) for an MCPTT emergency private call and optionally an MCPTT emergency alert, the originator will consider a SIP 200 (OK) response populated in this manner as confirmation that its request(s) for an upgrade to an MCPTT emergency private call and optionally an MCPTT emergency alert were accepted by the controlling function.

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

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

Upon receiving a SIP ACK to the SIP 200 (OK) response sent towards the inviting MCPTT client, and the SIP 200 (OK) response was sent with the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.18:

The controlling MCPTT function shall forward any other SIP response that does not contain SDP, including any MIME bodies contained therein, along the signalling path to the originating network according to 3GPP TS 24.229 [4].

11.1.1.4.4 Receiving a SIP re-INVITE for cancellation of emergency private call

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

Upon receiving a SIP re-INVITE request with an emergency indication set to a value of "false", the controlling MCPTT function:

1) shall validate that the received SDP offer includes at least one media stream for which the media parameters and at least one codec or media format is acceptable by the controlling MCPTT function and if not, reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

2) shall validate the request as described in subclause 6.3.3.1.17;

3) if the SIP re-INVITE request contains an unauthorised request for an MCPTT emergency private call cancellation as determined by subclause 6.3.3.1.13.4:

   a) shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response;

   b) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in annex F.1 with an <emergency-ind> element set to a value of "true";

   c) if the SIP re-INVITE request contains an alert indication set to "false" and this is an unauthorised request for an MCPTT emergency alert cancellation as specified in subclause 6.3.3.1.13.3, shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element set to "true; and

   d) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

4) shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response if a Resource-Priority header field is included in the received SIP re-INVITE request set to the value configured for emergency calls, and skip the remaining steps; and

5 if the SIP re-INVITE request contains an authorised request for an MCPTT emergency private call cancellation as determined by subclause 6.3.3.1.13.4:

a) shall clear the cache of the MCPTT ID of the originator of the MCPTT emergency private call that is no longer in an in-progress emergency private call state with the targeted MCPTT user; and

b) if the SIP re-INVITE request contains an alert indication set to "false" and this is an authorised request for an MCPTT emergency alert cancellation meeting the conditions specified in subclause 6.3.3.1.13.3:

i) if the received SIP re-INVITE request contains an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body,, shall clear the cache of the MCPTT ID of MCPTT user identified by the <originated-by> element as having an outstandingMCPTT emergency alert; and

ii) if the received SIP re-INVITE request does not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, clear the cache of the MCPTT ID of the sender of the SIP re-INVITE request as having an outstanding MCPTT emergency alert;

6) shall send a SIP re-INVITE request towards the MCPTT user listed in the MIME resource-lists body of received SIP re-INVITE request as specified in subclause 11.1.1.4.6.

Upon receiving a SIP 200 (OK) response for the SIP re-INVITE request and if the SIP response has not yet been sent to the inviting MCPTT client, the controlling MCPTT function:

1) shall generate a SIP 200 (OK) response to the SIP re-INVITE request as specified in the subclause 6.3.3.2.3 before continuing with the rest of the steps;

2) shall include in the SIP 200 (OK) response an SDP answer to the SDP offer in the incoming SIP re-INVITE request as specified in the subclause 6.3.3.2.2;

3) if the received SIP re-INVITE request contains an alert indication set to a value of "false" and this is an unauthorised request for an MCPTT emergency alert cancellation as specified in subclause 6.3.3.1.13.3, shall include in the SIP 200 (OK) response the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4.

NOTE: When a SIP 200 (OK) response sent to the originator as a response to a SIP INVITE request that contained authorised request(s) for an MCPTT emergency private call cancellation and optionally an MCPTT emergency alert cancellation, the originator will consider a SIP 200 (OK) response populated in this manner as confirmation that its request(s) for cancellation of an MCPTT emergency private call and optionally an MCPTT emergency alert were accepted by the controlling function.

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

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

Upon receiving a SIP ACK to the SIP 200 (OK) response sent towards the inviting MCPTT client, and the SIP 200 (OK) response was sent with the warning text set to "149 SIP INFO request pending" in a Warning header field as specified in subclause 4.4, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.18.

The controlling MCPTT function shall forward any other SIP response that does not contain SDP, including any MIME bodies contained therein, along the signalling path to the originating network according to 3GPP TS 24.229 [4].

11.1.1.4.5 Sending a SIP re-INVITE for upgrade to emergency private call

This subclause describes the procedures for sending a re-INVITE request to an MCPTT user in an MCPTT private call for the purpose of upgrading the session to an emergency private call session. The procedure is initiated by the controlling MCPTT function as the result of an action in subclause 11.1.1.4.3.

The controlling MCPTT function:

1) shall generate a SIP re-INVITE request as specified in subclause 6.3.3.1.9;

2) if the received SIP re-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 re-INVITE request;

3) if the received SIP re-INVITE request contains an authorised request for an MCPTT emergency private call as determined by subclause 6.3.3.1.13.2:

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

   b) if the received SIP INVITE request contains an alert indication set to a value of "true" and this is an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, perform the procedures specified in subclause 6.3.3.1.12; and

   c) if the received SIP INVITE request did not contain an alert indication or contains an alert indication set to a value of "true" and is not an authorised request for an MCPTT emergency alert meeting the conditions specified in subclause 6.3.3.1.13.1, shall set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false";

4) shall include a Resource-Priority header field populated with the values for an MCPTT emergency private call as specified in subclause 6.3.3.1.19, if the received SIP re-INVITE request contains an authorised request for an MCPTT emergency private call as determined in step 2 above; and

5) shall send the SIP re-INVITE request towards the core network according to 3GPP TS 24.229 [4].

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

1) shall cache the contact received in the Contact header field.

11.1.1.4.6 Sending a SIP re-INVITE for cancellation of emergency private call

This subclause describes the procedures for sending a re-INVITE request to an MCPTT user in an MCPTT emergency private call for the purpose of downgrading the session to a normal priority private call session. The procedure is initiated by the controlling MCPTT function as the result of an action in subclause 11.1.1.4.4.

The controlling MCPTT function:

1) shall generate a SIP re-INVITE request as specified in subclause 6.3.3.1.9;

2) if the received SIP re-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 re-INVITE request.

3) if the received SIP re-INVITE request contains an authorised request for an MCPTT emergency private call cancellation as determined by subclause 6.3.3.1.13.4:

   a) shall set the <emergency-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false";

   b) if the received SIP INVITE request contains an alert indication set to a value of "false" and this is an authorised request for an MCPTT emergency alert cancellation meeting the conditions specified in subclause 6.3.3.1.13.3:

      i) shall set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false"; and

      ii) if the received SIP request contains an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, copy the contents of the received <originated-by> element to an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP re-INVITE request;

   c) if the received SIP INVITE request contains an alert indication set to a value of "false" and is not an authorised request for an MCPTT emergency alert cancellation meeting the conditions specified in subclause 6.3.3.1.13.3, shall set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "true";

4) shall include a Resource-Priority header field populated with the values for a normal MCPTT private call as specified in subclause 6.3.3.1.19, if the received SIP re-INVITE request contains an authorised request for an MCPTT emergency private call cancellation as determined in step 3 above; and

5) shall send the SIP re-INVITE request towards the core network according to 3GPP TS 24.229 [4].

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

1) shall cache the contact received in the Contact header field.

11.1.2 Private call without floor control and first-to-answer call without floor control

11.1.2.1 General

Subclause 11.1.2 specifies the MCPTT client procedures, participating MCPTT function procedures and controlling MCPTT function procedures for on-network private calls without floor control and first-to-answer calls without floor control. The procedures in subclause 11.1.2 refer to the on-network private calls with floor control procedures and first-to-answer calls with floor control procedures in subclause 11.1.1 citing the differences.

11.1.2.2 MCPTT client procedures

When the MCPTT user wants to make an on-demand private call without floor control or first-to-answer call without floor control, the MCPTT client shall follow the procedures in subclause 11.1.1.2.1.1 with the following exceptions:

1) in step 12) of subclause 11.1.1.2.1.1, the MCPTT client shall not offer a media-level section for a media-floor control entity; and

2) step 13) of subclause 11.1.1.2.1.1 shall be ignored.

When the MCPTT user wants to make a private call without floor control or first-to-answer call without floor control using a pre-established session, the MCPTT client shall follow the procedures in subclause 11.1.1.2.2.1 with the following exceptions:

1) step 8 c) i) is re-written as: if the SDP parameters of the pre-established session contain a media-level section of a media-floor control entity or if end-to-end security is required for the private call, an application/sdp MIME body containing the SDP parameters of the pre-established session according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.1. If the pre-established session was established with implicit floor control, then the application/sdp MIME body shall not contain the implicit floor request as specified in subclause 6.4; and

2) step 9a) is re-written as: if the SDP parameters of the pre-established session contain a media-level section of a media-floor control entity, an application/sdp MIME body containing the SDP parameters of the pre-established session according to 3GPP TS 24.229 [4] with the clarifications given in subclause 6.2.1. If the pre-established session was established with implicit floor control, then the application/sdp MIME body shall not contain the implicit floor request as specified in subclause 6.4.

Upon receipt of an initial SIP INVITE request for the private call or first-to-answer call with an SDP offer not including a media-level section for a media-floor control entity, the MCPTT client shall consider it as the request for private call without floor control and shall follow the procedures as specified in subclause 11.1.1.2.1.2 for on-demand session and subclause 11.1.1.2.2.2 for pre-established session.

11.1.2.3 Participating MCPTT function procedures

11.1.2.3.1 Originating procedures

Upon receipt of a "SIP INVITE request for originating participating MCPTT function" or "SIP REFER request for a pre-established session" for the private call or first-to-answer call with SDP offer not including media-level section for media-floor control entity, the participating MCPTT function shall consider it as the request for the private call without floor control or first-to-answer call without floor control and shall follow the procedures as specified in subclause 11.1.1.3.1.1 for an on-demand session and shall follow the procedures as specified in subclause 11.1.1.3.1.2 for initiation using a pre-established session.

11.1.2.3.2 Terminating procedures

Upon receipt of a "SIP INVITE request for terminating participating MCPTT function" for the private call or first-to-answer call with SDP offer not including media-level section for media-floor control entity, the participating MCPTT

shall consider it as the request for the private call without floor control or first-to-answer call without floor control and shall follow the procedures as specified in subclause 11.1.1.3.2.

11.1.2.4 Controlling MCPTT function procedures

11.1.2.4.1 Originating procedures

The controlling MCPTT function shall follow the procedures as specified in subclause 11.1.1.4.1.

11.1.2.4.2 Terminating procedures

Upon receiving of a "SIP INVITE request for controlling MCPTT function of a private call" or a "SIP INVITE request for controlling MCPTT function of a first-to-answer call", with SDP offer not including media-level section for media-floor control entity, the controlling MCPTT function shall consider it as the request for the private call without floor control or first-to-answer call without floor control, and shall follow the procedures as specified in subclause 11.1.1.4.2.

11.1.3 Ending the private call initiated by MCPTT client

11.1.3.1 MCPTT client procedures

11.1.3.1.1 On-demand private call

11.1.3.1.1.1 Client originating procedures

Upon receiving a request from an MCPTT user to release an MCPTT private call session established using on-demand session signalling, the MCPTT client shall follow the procedures as specified in subclause 6.2.5.1.

11.1.3.1.1.2 Client terminating procedures

Upon receiving a SIP BYE request for private call session, the MCPTT client shall follow the procedures as specified in subclause 6.2.6.

11.1.3.1.2 Private call using pre-established session

11.1.3.1.2.1 Client originating procedures

Upon receiving a request from an MCPTT user to release an MCPTT private call within a pre-established session, the MCPTT client shall follow the procedures as specified in subclause 6.2.5.2.

11.1.3.1.2.2 Client terminating procedures

The MCPTT client shall follow the procedures for terminating of request for MCPTT private call release as specified in subclause 6.2.6.

11.1.3.2 Participating MCPTT function procedures

11.1.3.2.1 Originating procedures

11.1.3.2.1.1 Receipt of SIP BYE request for on-demand private call

Upon receiving from the MCPTT client a SIP BYE request the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.1.6.

11.1.3.2.1.2 Receipt of REFER "BYE" request for private call using pre-established session

Upon receiving from the MCPTT client a SIP REFER request when using a pre-established session with the "method" SIP URI parameter set to value "BYE" in the URI in the Refer-To header field the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.1.7.

11.1.3.2.2 Terminating procedures

11.1.3.2.2.1 Receipt of SIP BYE request for private call on-demand

Upon receiving a SIP BYE request from the controlling MCPTT function, the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.2.8.1.

11.1.3.2.2.2 Receipt of SIP BYE request when ongoing pre-established session

Upon receiving a SIP BYE request from the controlling MCPTT function and if the MCPTT session id refers to an MCPTT user that has a pre-established session with the participating MCPTT function, the participating MCPTT function:

1) shall interact with the media plane as specified in subclause 9.3 in 3GPP TS 24.380 [5] for disconnecting the media plane resources towards the controlling MCPTT function;

2) shall send a SIP 200 (OK) response to the controlling MCPTT function;

3) shall interact with the media plane as specified in subclause 9.3 in 3GPP TS 24.380 [5] for disconnecting media plane resources towards the MCPTT client from the media plane resources towards the controlling MCPTT function; and

4) shall maintain the pre-established session towards the MCPTT client.

11.1.3.3 Controlling MCPTT function procedures

11.1.3.3.1 Terminating procedures

Upon receiving a SIP BYE request the controlling MCPTT function shall follow the procedures as specified in subclause 6.3.3.2.4.

11.1.4 Ending the private call initiated by the MCPTT server

11.1.4.1 General

This subclause describes the procedures of each functional entity for ending the private call initiated by the MCPTT server.

NOTE: For private call without floor control, ending the private call is initiated only by the MCPTT client.

11.1.4.2 MCPTT client procedures

Upon receiving a SIP BYE request for private call session, the MCPTT client shall follow the procedures as specified in subclause 6.2.6.

11.1.4.3 Participating MCPTT function procedures

11.1.4.3.1 Originating procedures

When the MCPTT session for private call needs to be released as specified in subclause 6.3.8.2, the participating MCPTT function shall follow the procedures in subclause 6.3.3.1.5.

11.1.4.3.2 Terminating procedures

11.1.4.3.2.1 Receipt of SIP BYE request for private call on-demand

Upon receiving a SIP BYE request from the controlling MCPTT function, the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.2.8.1.

11.1.4.3.2.2 Receipt of SIP BYE request when ongoing pre-established session

Upon receiving a SIP BYE request from the controlling MCPTT function and if the MCPTT session id refers to an MCPTT user that has a pre-established session with the participating MCPTT function, the participating MCPTT function shall follow the procedures in subclause 11.1.3.2.2.2.

11.1.4.4 Controlling MCPTT function procedures

When the MCPTT session for private call needs to be released as specified in subclause 6.3.8.2, the controlling MCPTT function shall follow the procedures in subclause 6.3.3.1.5.

11.1.5 Private call call-back

11.1.5.1 General

Subclause 11.1.5 describes the MCPTT client procedures, the participating MCPTT function procedures and the controlling MCPTT function procedures for private call call-back.

In the procedures in subclause 11.1.5.2:

- the term "requesting MCPTT client" is used to refer to the client that initiates a private call call-back request, initiates a private call call-back cancel request or receives a private call call-back fulfilment;
- the term "requesting MCPTT user" is used to refer to the MCPTT user that requests a private call call-back or requests a private call call-back cancel;
- the term "target MCPTT client" is used to refer to the client that generates a private call call-back response, generates a private call call-back cancel response or initiates a private call call-back fulfilment; and
- the term "target MCPTT user" is used to refer to the MCPTT user that is targeted for a private call call-back request or a private call call-back cancel request,

The requesting MCPTT client needs to store the MCPTT ID of the target MCPTT user together with state information as specified in Table G.13-1. In the procedures in subclause 11.1.5.2, the notation {MCPTT-ID, private call call-back requesting client state} is used to describe the information that the requesting MCPTT client stores.

The target MCPTT client needs to store the MCPTT ID of the requesting MCPTT user together with state information as specified in Table G.13-2. Additionally, for a private call call-back request, the target MCPTT client needs to store the urgency of the request and the time of the request. In the procedures in subclause 11.1.5.2, the notation {MCPTT ID, private call call-back target client state, urgency, time-of-request} is used to describe the information that the target MCPTT client stores.

The {MCPTT-ID, private call call-back requesting client state} entry on the requesting MCPTT client is known as the "PCCB requesting client entry".

The {MCPTT ID, private call call-back target client state, urgency, time-of-request} entry on the target MCPTT client is known as the "PCCB target client entry".

When a private call call-back request is cancelled or when a private call call-back is fulfilled, the "PCCB requesting client entry" is deleted on the requesting MCPTT client and the "PCCB target client entry" is deleted on the target MCPTT client.

11.1.5.2 MCPTT client procedures

11.1.5.2.1 Requesting client procedures for call-back requests

Upon receiving a request from the MCPTT user to send a private call call-back request, if the <allow-request-private-call-call-back> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.384 [50]) or is set to a value of "false", the MCPTT client shall inform the MCPTT user and shall exit this procedure.

Upon receiving a request from the MCPTT user to send a private call call-back cancel request, if the <allow-cancel-private-call-call-back> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.384 [50]) or is set to a value of "false", the MCPTT client shall inform the MCPTT user and shall exit this procedure.

Upon receiving a request from the requesting MCPTT user to send a private call call-back request or to send a private call call-back cancel request, that has been authorised successfully by the requesting MCPTT client, the MCPTT client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] with the clarifications given below.

The MCPTT client:

1) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP MESSAGE request;

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

3) may include a P-Preferred-Identity header field in the SIP MESSAGE request containing a public user identity as specified in 3GPP TS 24.229 [4];

4) shall set the Request-URI to the public service identity identifying the participating MCPTT function serving the MCPTT user;

5) shall include in an application/resource-lists+xml MIME body, the MCPTT ID of the targeted MCPTT user, according to rules and procedures of IETF RFC 5366 [20];

6) shall include an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <anyExt> element containing:

   a) if the request is a private call call-back request:

      i) the <request-type> set to a value of "private-call-call-back-request>;

      ii) the <urgency-ind> set to a value of "low", "normal" or "high" to indicate the urgency of the call-back request; and

      iii) the <time-of-request> set to the date and time of the request using the format specified in clause F.1.3; and

   b) if the request is a private call call-back cancel request, the <request-type> set to a value of "private-call-call-back-cancel-request";

7) shall store a "PCCB requesting client entry" containing the MCPTT ID of the targeted user and:

   a) if the request is a private call call-back request, shall set the private call call-back requesting client state to "PCCB-I2: confirm-pending"; and

   b) if the request is a private call call-back cancel request, shall set the private call call-back requesting client state to "PCCB-I4: cancel-pending"; and

8) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

On receiving a SIP 4xx response a SIP 5xx response or a SIP 6xx response to the SIP MESSAGE request in step 8), the MCPTT client shall set the private call call-back requesting client state of the "PCCB requesting client entry" matching

the MCPTT ID of the targeted MCPTT user, to "PCCB-I1: no-call-back", shall delete the "PCCB requesting client entry" and shall exit this procedure.

Upon receiving a "SIP MESSAGE request for private call call-back response for terminating client" with an <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body set to an MCPTT-ID matching a "PCCB requesting client entry" stored on the client, if the private call call-back requesting client state is set to "PCCB-I2: confirm-pending", then the MCPTT client shall set the private call call-back requesting client state to "PCCB-I3: confirmed".

Upon receiving a "SIP MESSAGE request for private call call-back cancel response for terminating client" with an <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body set to the an MCPTT-ID matching a "PCCB requesting client entry" entry stored on the client, if the private call call-back requesting client state is set to "PCCB-I4: cancel-pending", then the MCPTT client set the private call call-back requesting client state to "PCCB-I1: no-call-back" and shall delete the "PCCB requesting client entry" associated with the target MCPTT user.

11.1.5.2.2 Target client procedures for handling call-back requests

Upon receiving a "SIP MESSAGE request for private call call-back request for terminating client", the MCPTT client:

1) shall store a "PCCB target client entry" entry with:

   a) the MCPTT ID set to the MCPTT ID contained in the <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body;

   b) the private call call-back receiving client state set to "PCCB-I2: private-call-pending";

   c) the urgency set to the value of the <urgency-ind> element in the application/vnd.3gpp.mcptt-info+xml MIME body; and

   d) the time-of-request set to the value of the <time-of-request> element in the application/vnd.3gpp.mcptt-info+xml MIME body; and

2) shall notify the user of the stored information related to the private call call back request.

Upon receiving a "SIP MESSAGE request for private call call-back cancel request for terminating client" where the "PCCB target client entry" associated with the MCPTT ID in the <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body contains a private call call-back requesting client state set to "PCCB-R2: private-call-pending", the MCPTT client shall set the private call call-back requesting client state to "PCCB-R1: no-call-back" and shall delete the "PCCB target client entry" associated with the requesting MCPTT user.

The MCPTT client:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33]:

2) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP MESSAGE request;

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

4) may include a P-Preferred-Identity header field in the SIP MESSAGE request containing a public user identity as specified in 3GPP TS 24.229 [4];

5) shall set the Request-URI in the SIP MESSAGE request to the public service identity identifying the participating MCPTT function serving the MCPTT user;

6) shall include in an application/resource-lists+xml MIME body, the MCPTT ID contained in the <mcptt-calling-user-id> element in the application/ vnd.3gpp.mcptt-info+xml MIME body of the received SIP MESSAGE request;

7) shall include an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <anyExt> element containing:

a) if the received SIP MESSAGE was a "SIP MESSAGE request for private call call-back request for terminating MCPTT client", the <response-type> element set to a value of "private-call-call-back-response"; and

b) if the received SIP MESSAGE was a "SIP MESSAGE request for private call call-back cancel request for terminating MCPTT client", the <response-type> element set to a value of "private-call-call-back-cancel-response"; and

8) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

11.1.5.2.3 Private call call-back fulfilment

When the target MCPTT user wants to make a private call call-back, the target MCPTT client shall initiate a private call in manual commencement mode towards the requesting MCPTT client using the MCPTT ID of the requesting MCPTT user as found in the "PCCB target client entry" stored on the UE, by following the procedures in:

1) subclause 11.1.1.2.1.1 or subclause 11.1.1.2.2.1 for private call with floor control; or

2) subclause 11.1.2.2 for private call without floor control;

Upon sending a SIP 200 (OK) response to the request for establishment of a private call as specified in subclause 11.1.1.2.1.1, subclause 11.1.1.2.2.1 or subclause 11.1.2.2, if the "PCCB requesting client entry" of the target MCPTT user contains a private call call-back requesting client state set to "PCCB-I3: confirmed", then the requesting MCPTT client shall set the private call call-back requesting client state to "PCCB-I1: no-call-back" and shall delete the "PCCB requesting client entry" associated with the target MCPTT user.

Upon receiving a SIP 2xx response to the SIP INVITE request or SIP REFER request for establishment of the private call, as specified in subclause 11.1.1.2.1.1, subclause 11.1.1.2.2.1 or subclause 11.1.2.2, if the "PCCB target client entry" of the requesting MCPTT user contains a private call call-back target client state set to "PCCB-R2: private-call-pending", then the target MCPTT client shall set the private call call-back target client state to "PCCB-R1: no-call-back" and shall delete the "PCCB target client entry" associated with the requesting MCPTT user.

11.1.5.3 Participating MCPTT function procedures

11.1.5.3.1 Originating procedures

Upon receiving a "SIP MESSAGE request for private call call-back for originating 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 MESSAGE 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 skip the rest of the steps;

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

NOTE: 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 the "SIP MESSAGE request for private call call-back for originating participating MCPTT function" contains the <request-type> element set to a value of "private-call-call-back-request", and the <allow-request-private-call-call-back> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.384 [50]) or is set to a value of "false", shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "151 user not authorised to make a private call call-back request" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps in this subclause;

4) if the "SIP MESSAGE request for private call call-back for originating participating MCPTT function" contains the <request-type> element set to a value of "private-call-call-back-cancel-request", and the <allow-cancel-private-call-call-back> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.384 [50]) or is set to a value of "false", shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "152 user not authorised

to make a private call call-back cancel request" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps in this subclause;

5) shall determine the public service identity of the controlling MCPTT function for the private call call-back service for the MCPTT user;

6) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

7) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the controlling MCPTT function associated with the private call call-back service for the MCPTT user;

8) shall copy the contents of the application/vnd.3gpp. mcptt-info+xml MIME body in the received SIP MESSAGE request into an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 included in the outgoing SIP MESSAGE request;

9) shall set the <mcptt-calling-user-id> element of the <mcpttinfo> element containing the <mcptt-Params> element to the MCPTT ID determined in step 2) above;

10) shall copy the contents of the application/resource-lists MIME body in the received SIP MESSAGE request into an application/resource-lists MIME body in the outgoing SIP MESSAGE request;

11) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP MESSAGE request;

12) 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];

13) 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];

14) 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 MESSAGE request; and

15) shall send the SIP MESSAGE request as specified to 3GPP TS 24.229 [4].

Upon receipt of a SIP 2xx response in response to the SIP MESSAGE request sent in step 13), the participating MCPTT function shall generate a SIP 200 (OK) response and forward the SIP 200 (OK) response to the MCPTT client.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request, shall forward the error response to the MCPTT client.

11.1.5.3.2 Terminating procedures

Upon receiving a "SIP MESSAGE request for private call call-back 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 MESSAGE 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 skip the rest of the steps;

2) 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 MESSAGE request to retrieve the binding between the MCPTT ID and public user identity;

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

4) shall generate an outgoing SIP MESSAGE request as specified in subclause 6.3.2.2.11;

5) 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; and

6) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the participating MCPTT function shall forward the SIP 2xx response to the controlling MCPTT function.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request, shall forward the response to the controlling MCPTT function.

11.1.5.4 Controlling MCPTT function procedures

Upon receiving a:

- "SIP MESSAGE request for private call call-back request for controlling MCPTT function";
- "SIP MESSAGE request for private call call-back cancel request for controlling MCPTT function"; or
- "SIP MESSAGE request for private call call-back responses for controlling MCPTT function";

the controlling 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 MESSAGE request with a SIP 500 (Server Internal Error) response. The controlling 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;

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

3) if the incoming SIP MESSAGE request does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

4) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

5) 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];

6) 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];

7) shall copy the contents of the application/vnd.3gpp. mcptt-info+xml MIME body in the received SIP MESSAGE request into an application/vnd.3gpp.mcptt-info+xml MIME body included in the outgoing SIP MESSAGE request;

8) shall copy the MCPTT ID of the MCPTT user listed in the MIME resources body of the incoming SIP MESSAGE request, into the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the outgoing SIP MESSAGE request;

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

10) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

11) shall copy the public user identity of the calling MCPTT user from the P-Asserted-Identity header field of the incoming SIP MESSAGE request into the P-Asserted-Identity header field of the outgoing SIP MESSAGE request; and

12) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [4].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the controlling MCPTT function shall generate a SIP 200 (OK) response and forward the SIP 200 (OK) response to the originating participating MCPTT function.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the SIP MESSAGE request, controlling MCPTT function shall forward the error response to the originating participating MCPTT function.

11.1.6 Ambient listening call

11.1.6.1 General

Subclause 11.1.6 specifies the MCPTT client procedures, participating MCPTT function procedures and controlling MCPTT function procedures for on-network ambient listening calls. The procedures as specified are applicable to both locally initiated and remotely initiated ambient listening call.

The procedures for originating an ambient listening call are initiated by the MCPTT user at the MCPTT client in the following circumstances:

- an authorised MCPTT user initiates an ambient listening call in order to listen to the terminating user; or
- an authorised MCPTT user initiates an ambient listening call in order to be listened to by the terminating user.

The procedures for releasing an ambient listening call are initiated by the MCPTT user at the MCPTT client in the following circumstances:

- a listening MCPTT user initiates the ambient listening call release; or
- a listened-to MCPTT user who was the originator of the ambient listening call initiates the ambient listening call release.

The procedures for releasing an ambient listening call by the controlling MCPTT function are initiated in the following circumstances:

- can be triggered by the MCPTT administrator by a mechanism outside of the scope of the standard; or
- can be triggered by a call terminating event occurring at the controlling MCPTT function such as a timer expiration.

11.1.6.2 MCPTT client procedures

11.1.6.2.1 On-demand ambient listening call

11.1.6.2.1.1 Client originating procedures for remote-initiated call

Upon receiving a request from the MCPTT user to originate a remote initiated ambient listening call, if the <allow-request-remote-initiated-ambient-listening> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false", the MCPTT client shall inform the MCPTT user and shall exit this procedure.

Upon receiving a request from the MCPTT user to originate a locally initiated ambient listening call, if the <allow-request-locally-initiated-ambient-listening> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false", the MCPTT client shall inform the MCPTT user and shall exit this procedure.

Upon receiving a request from an MCPTT user to establish an MCPTT ambient listening call that has been authorised successfully by the requesting MCPTT client, the MCPTT client shall generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [4], with the clarifications given below.

The MCPTT client:

1) shall set the Request-URI of the SIP INVITE request to a public service identity of the participating MCPTT function serving the MCPTT user;

2) may include a P-Preferred-Identity header field in the SIP INVITE request containing a public user identity as specified in 3GPP TS 24.229 [4];

3) shall include the g.3gpp.mcptt media feature tag and the g.3gpp.icsi-ref media feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt" in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [16];

4) 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];

5) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP INVITE request;

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

7) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <session-type> element set to a value of "ambient-listening";

8) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body an <ambient-listening-type> element set to a value of:

   a) "local-init", if the MCPTT user has requested a locally initiated ambient listening call; or

   b) "remote-init", if the MCPTT user has requested a remotely initiated ambient listening call;

9) shall insert in the SIP INVITE request a MIME resource-lists body with the MCPTT ID of the targeted MCPTT user, according to rules and procedures of IETF RFC 5366 [20];

NOTE 1: the targeted MCPTT user is the listened-to MCPTT user in the case of a remotely initiated ambient listening call or the listening MCPTT user in the case of a locally initiated listening call.

10) if an end-to-end security context needs to be established then:

   a) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [78];

   b) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [78];

   c) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect private call communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [78];

   d) shall encrypt the PCK to a UID associated to the MCPTT client using the MCPTT ID and KMS URI of the invited user and a time related parameter as described in 3GPP TS 33.180 [78];

   e) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [78];

   f) shall add the MCPTT ID of the originating MCPTT to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]; and

   g) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCPTT user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [78];

11) shall include an SDP offer according to 3GPP TS 24.229 [4] with the clarification given in subclause 6.2.1 and with a media stream of the offered media-floor control entity;

12) if this is a locally initiated ambient listening call, shall comply with the conditions for implicit floor control as specified in subclause 6.4;

13) if this is a remotely initiated ambient listening call, shall comply with the conditions for an implicit request to grant the floor to the terminating MCPTT client as specified in subclause 6.4;

14) shall include in the SIP INVITE request a Priv-Answer-Mode header field with the value "Auto" according to the rules and procedures of IETF RFC 5373 [18]; and

15) shall send the SIP INVITE request towards the participating MCPTT function according to 3GPP TS 24.229 [4].

Upon receiving a SIP 183(Session Progress) response to the SIP INVITE request the MCPTT client:

1) if the SIP 183(Session Progress) response includes an alert-info header field as specified in IETF RFC 3261 [24] and as updated by IETF RFC 7462 [77] set to a value of "<C:\dev\nullfile:///dev/null>" shall not give any indication of the progress of the call setup to the MCPTT user; and

NOTE 2: The alert-info header field having the value of "<C:\dev\nullfile:///dev/null>" is intended to result in having a "null" alert, i.e. an alert with no content or physical manifestation of any kind.

2) if this is a remotely initiated ambient listening call, may indicate the progress of the session establishment to the inviting MCPTT user.

Upon receiving a SIP 200 (OK) response to the SIP INVITE request the MCPTT client:

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

2) if this is a remotely initiated ambient listening call, shall notify the user that the call has been successfully established;

3) if this is a locally initiated ambient listening call, shall not provide any indication to the user that the call has been successfully established;

4) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body in the sent SIP INVITE request was set to a value of "local-init":

   a) shall cache the value of "listened-to MCPTT user" as the ambient listening client role for this call; or

   b) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body was set to a value of "remote-init" shall cache the value of "listening MCPTT user" as the ambient listening client role for this call; and

5) shall cache the value contained in the <ambient-listening-type> element of the application/vnd.3gpp.mcptt-info+xml MIME body set in step 8) as the ambient listening type of this call.

11.1.6.2.1.2 Client terminating procedures

Upon receipt of an initial SIP INVITE request, the MCPTT client shall follow the procedures for termination of multimedia sessions in the IM CN subsystem as specified in 3GPP TS 24.229 [4] with the clarifications below.

The MCPTT client:

1) may reject the SIP INVITE request if either of the conditions in step a) or b) are met:

   a) MCPTT client is already occupied in another session and the number of simultaneous sessions exceeds <MaxCall>, the maximum simultaneous MCPTT session for private call, as specified in TS 24.384 [50]; or

   b) MCPTT client does not have enough resources to handle the call;

   c) if neither condition a) nor b) are met, continue with the rest of the steps;

2) if the SIP INVITE request is rejected in step 1):

   a) shall respond towards the participating MCPTT function either with:

      i) an appropriate reject code as specified in 3GPP TS 24.229 [4] and warning texts as specified in subclause 4.4.2; or

      ii) with a SIP 480 (Temporarily unavailable) response not including warning texts if the user is authorised to restrict the reason for failure according to <allow-failure-restriction> as specified in 3GPP TS 24.384 [50]; and

   b) skip the rest of the steps of this subclause;

3) if the SDP offer of the SIP INVITE request contains an "a=key-mgmt" attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

   a) shall extract the MCPTT ID of the originating MCPTT from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78];

   b) shall convert the MCPTT ID to a UID as described in 3GPP TS 33.180 [78];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [78];

   d) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails, shall reject the SIP INVITE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and include warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4; and

   e) if the signature of the MIKEY-SAKKE I_MESSAGE was successfully validated:

      i) shall extract and decrypt the encapsulated PCK using the terminating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [78]; and

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [78];

NOTE 1: With the PCK successfully shared between the originating MCPTT client and the terminating MCPTT client, both clients are able to use SRTP/SRTCP to create an end-to-end secure session.

4) may check if a Resource-Priority header field is included in the incoming SIP INVITE request and may perform further actions outside the scope of this specification to act upon an included Resource-Priority header field as specified in 3GPP TS 24.229 [4];

5) if the received SIP INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <ambient-listening-type> element set to a value of "local-init", may display to the MCPTT user the MCPTT ID of the inviting MCPTT user;

6) shall perform the automatic commencement procedures specified in subclause 6.2.3.1.1;

NOTE 2: Auto-answer is the commencement mode for both participants in locally initiated and remotely initiated ambient listening calls.

7) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP INVITE request was set to a value of "remote-init":

   a) shall cache the value of "listened-to MCPTT user" as the ambient listening client role for this call; or;

   b) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body was set to a value of "local-init" " shall cache the value of "listening MCPTT user" as the ambient listening client role for this call;

8) if the received SIP INVITE request includes an alert-info header field as specified in IETF RFC 3261 [24] and as updated by IETF RFC 7462 [77] set to a value of "<file:///dev/null>" shall not give any indication of the progress of the call to the MCPTT user;

NOTE 3: The alert-info header field having the value of "<file:///dev/null>" is intended to result in having a "null" alert, i.e. an alert with no content or physical manifestation of any kind.

9) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body is set to a value of "local-init", should provide an indication to the MCPTT user that the ambient listening call is in progress; and

NOTE 4: The terminating user in a remotely initiated ambient listening is the listened-to MCPTT user and is intended to be totally unaware that their microphone is activated and a call is in progress.

10) shall cache as the ambient listening type for the call the value contained in the <ambient-listening-type> element of the application/vnd.3gpp.mcptt-info+xml MIME body contained in the received SIP INVITE request.

11.1.6.2.1.3 Client release origination procedure

Upon receiving a request from an MCPTT user to release an MCPTT ambient listening call:

The MCPTT client:

1) if the MCPTT client has not received a g.3gpp.mcptt.ambient-listening-call-release feature-capability indicator as described in clause D.3 in the Feature-Caps header field according to IETF RFC 6809 [60] in;

   a) a received SIP INVITE request for the ambient listening call; or

   b) a received SIP 200 (OK) response to a sent SIP INVITE request for the ambient listening call;

   then shall skip the rest of the steps;

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

3) shall generate a SIP BYE request according to rules and procedures of 3GPP TS 24.229 [4] and IETF RFC 6086 [64]; and

4) shall send the SIP BYE request within the dialog of the MCPTT ambient call session as specified in 3GPP TS 24.229 [4].

Upon receipt of the SIP 200 (OK) response to the SIP BYE request the MCPTT client:

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

2) if the cached ambient listening client role is equal to "listened-to MCPTT user", shall provide no indication that an ambient listening call has been terminated;

3) if the cached ambient listening client role is equal to "listening MCPTT user", may provide an indication to the MCPTT user that the ambient listening call has been terminated; and

4) shall clear the cache of the data stored as:

   a) ambient listening client role; and

   b) ambient listening type.

11.1.6.2.1.4 Client session release termination procedure

This subclause is referenced from other procedures.

Upon receipt of a SIP BYE request in the dialog of an ambient listening session, the MCPTT client:

1) shall comply with the procedures of subclause 6.2.6;

2) if the cached ambient listening client role is equal to "listened-to MCPTT user", shall provide no indication that an ambient listening call has been terminated;

3) if the cached ambient listening client role is equal to "listening MCPTT user", may provide an indication to the MCPTT user that the ambient listening call has been terminated; and

4) shall clear the cache of the data stored as:

   a) ambient listening client role; and

   b) ambient listening type.

11.1.6.2.2 Ambient listening call using pre-established session

11.1.6.2.2.1 Client originating procedures

Upon receiving a request from the MCPTT user to originate a remote initiated ambient listening call, if the <allow-request-remote-initiated-ambient-listening> element of the <ruleset> element is not present in the MCPTT user profile

document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false", the MCPTT client shall inform the MCPTT user and shall exit this procedure.

Upon receiving a request from the MCPTT user to originate a locally initiated ambient listening call, if the <allow-request-locally-initiated-ambient-listening> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false", the MCPTT client shall inform the MCPTT user and shall exit this procedure.

Upon receiving a request from an MCPTT user to establish an MCPTT ambient listening call that has been authorised successfully by the requesting MCPTT client within a pre-established session, the MCPTT client shall generate a SIP REFER request outside a dialog in accordance with the procedures specified in 3GPP TS 24.229 [4], IETF RFC 4488 [22] and IETF RFC 3515 [25] as updated by IETF RFC 6665 [26] and IETF RFC 7647 [27], with the clarifications given below.

If an end-to-end security context needs to be established the MCPTT client:

1) if necessary, shall instruct the key management client to request keying material from the key management server as described in 3GPP TS 33.180 [78];

2) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [78];

3) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect private call communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [78];

4) shall encrypt the PCK to a UID associated to the MCPTT client using the MCPTT ID of the invited user and a time related parameter as described in 3GPP TS 33.180 [78];

5) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [78];

6) shall add the MCPTT ID of the originating MCPTT to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]; and

7) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCPTT user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [78].

The MCPTT client populates the SIP REFER request as follows:

1) shall include the Request-URI set to the public service identity identifying the pre-established session on the MCPTT server serving the MCPTT user;

2) shall include the Refer-Sub header field with value "false" according to rules and procedures of IETF RFC 4488 [22];

3) shall include the Supported header field with value "norefersub" according to rules and procedures of IETF RFC 4488 [22];

4) shall include the option tag "multiple-refer" in the Require header field;

5) may include a P-Preferred-Identity header field in the SIP REFER request containing a public user identity as specified in 3GPP TS 24.229 [4];

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

7) shall set the Refer-To header field of the SIP REFER request as specified in IETF RFC 3515 [25] with a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [20], and with the Content-ID header field set to this "cid" URL.

8) shall include in the application/resource-lists MIME body a single <entry> element containing a "uri" attribute set to the MCPTT ID of the targeted user, extended with hname "body" parameter containing:

   a) an application/vnd.3gpp.mcptt-info MIME body containing:

i) a <session-type> element set to "ambient-listening";

ii) if the MCPTT user has requested a locally initiated ambient listening call, an <ambient-listening-type> element set to a value of "local-init"; or

iii) if the MCPTT user has requested a remotely initiated ambient listening call, an <ambient-listening-type> element set to a value of "remote-init";

b) a Priv-Answer-Mode header field with the value "Auto" according to the rules and procedures of IETF RFC 5373 [18];

c) if the SDP parameters of the pre-established session do not contain a media-level section of a media-floor control entity or if end-to-end security is required for the ambient listening call, an application/sdp MIME body containing the SDP parameters of the pre-established session according to 3GPP TS 24.229 [4] with the clarification given in subclause 6.2.1;

d) if this is a locally initiated ambient listening call, shall comply with the conditions for implicit floor control as specified in subclause 6.4; and

e) if this is a remotely initiated ambient listening call, shall comply with the conditions for an implicit request to grant the floor to the terminating MCPTT client as specified in subclause 6.4; and

Editor's Note [CT1#103, C1-171322]: A mechanism (TBD) is needed to automatically grant the floor to the terminating user in the case of a remotely initiated ambient listening call.

9) shall include a Target-Dialog header field as specified in IETF RFC 4538 [23] identifying the pre-established session.

Upon receiving a final SIP 2xx response to the SIP REFER request the MCPTT client:

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

2) if this is a locally initiated ambient listening call, shall not provide any indication to the user that the call setup is in progress.

On call establishment by interaction with the media plane as specified in subclause 9.2.2 of 3GPP TS 24.380 [5] if the sent SIP REFER request the MCPTT client:

1) if the MCPTT user has requested a locally initiated ambient listening call shall provide no indication to the MCPTT user that the ambient listening call has been successfully established; and

2) if the MCPTT user has requested a remotely initiated ambient listening call shall provide an indication to the MCPTT user that the ambient listening call has been successfully established.

3) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body in the sent SIP REFER request was set to a value of "local-init":

a) shall cache the value of "listened-to MCPTT user" as the ambient listening client role for this call; or

b) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body was set to a value of "remote-init" shall cache the value of "listening MCPTT user" as the ambient listening client role for this call; and

4) shall cache the value contained in the <ambient-listening-type> element of the application/vnd.3gpp.mcptt-info+xml MIME body set in step 8) as the ambient listening type of this call.

11.1.6.2.2.2 Client terminating procedures

The MCPTT client shall follow the procedures for termination of multimedia sessions for ambient listening calls as specified in subclause 11.1.6.2.1.2.

NOTE: The terminating MCPTT client in an ambient listening call receives a SIP INVITE request with Replaces header field when using a pre-established session.

11.1.6.2.2.3 Client release origination procedure

Upon receiving a request from an MCPTT user to release an MCPTT ambient listening call when using a pre-established MCPTT session:

The MCPTT client:

1) if the MCPTT client has not received a g.3gpp.mcptt.ambient-listening-call-release feature-capability indicator as described in clause D.3 in the Feature-Caps header field according to IETF RFC 6809 [60] in;

   a) a received SIP INVITE request for the ambient listening call; or

   b) a received SIP 200 (OK) response to a sent SIP INVITE request or SIP REFER request for the ambient listening call;

   then shall skip the rest of the steps; and

2) shall perform the actions specified in subclause 6.2.5.2.

If the procedures of subclause 6.2.5.2 were successful:

1) if the cached ambient listening client role is equal to "listened-to MCPTT user", shall provide no indication that an ambient listening call has been terminated;

2) if the cached ambient listening client role is equal to "listening MCPTT user", may provide an indication to the MCPTT user that the ambient listening call has been terminated; and

3) shall clear the cache of the data stored as:

   a) ambient listening client role; and

   b) ambient listening type.

11.1.6.2.2.4 Reception of SIP INFO request with release-reason

Upon receiving a SIP INFO request containing an application/vnd.3gpp.mcptt-info+xml MIME body containing a <release-reason> element, the MCPTT client:

1) if the cached ambient listening client role is equal to "listened-to MCPTT user", shall provide no indication that an ambient listening call is being terminated;

2) if the cached ambient listening client role is equal to "listening MCPTT user", should provide an indication to the MCPTT user that an ambient listening call is being terminated;

3) shall generate and send a SIP 200 OK response to the SIP INFO request according to 3GPP TS 24.229 [4]; and

4) shall comply with the procedures of subclause 11.1.6.2.2.5.

11.1.6.2.2.5 Client session release termination procedure

This subclause is referenced from other procedures.

Upon receiving an interaction with the media plane indicating release of the ambient listening call but preservation of the pre-established session as specified in subclause 9.2 of 3GPP TS 24.380 [5], the MCPTT client:

1) if the cached ambient listening client role is equal to "listened-to MCPTT user", shall provide no indication that an ambient listening call has been terminated;

2) if the cached ambient listening client role is equal to "listening MCPTT user", may provide an indication to the MCPTT user that the ambient listening call has been terminated; and

3) shall clear the cache of the data stored as:

   a) ambient listening client role; and

   b) ambient listening type.

11.1.6.3 Participating MCPTT function procedures

11.1.6.3.1 Originating procedures

11.1.6.3.1.1 On-demand ambient listening call

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 "ambient-listening", 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 for originating participating MCPTT function" 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;

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 user;

NOTE: 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 the participating MCPTT function cannot find a binding between the public user identity and an MCPTT ID or if the validity period of an existing binding has expired, then the participating MCPTT function shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

4) if the <ambient-listening-type> element of the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP INVITE request is set to a value of:

   a) "remote-init" and an <allow-request-remote-initiated-ambient-listening> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false"; or

   b) "local-init" and an <allow-request-locally-initiated-ambient-listening> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false";

   then shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response, with warning text set to "154 The MCPTT user is not authorised to make an ambient listening call" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

5) shall determine the public service identity of the controlling MCPTT function for the ambient listening call service associated with the originating user's MCPTT ID identity. If the participating MCPTT function is unable to identify the controlling MCPTT function for the ambient listening call service associated with the originating user's MCPTT ID identity, it shall reject the SIP INVITE request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

6) if the incoming SIP INVITE request does not contain an application/resource-lists MIME body or contains an application/resource-lists MIME body with more than one <entry> element, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

7) if the <allow-private-call> element of the <ruleset> element is not present in the MCPTT user profile document on the participating MCPTT function or is present with the value "false" (see the MCPTT user profile document in 3GPP TS 24.484 [50]), indicating that the user identified by the MCPTT ID is not authorised to initiate private calls, shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response, with warning text set to "107 user not authorised to make private calls" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

8) if the <PrivateCall> element exists in the MCPTT user profile document with one or more <entry> elements (see the MCPTT user profile document in 3GPP TS 24.484 [50]) and:

   a) if the "uri" attribute of the <entry> element of the application/resource-lists MIME body does not match with one of the <entry> elements of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]); and

   b) if configuration is not set in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) that allows the MCPTT user to make a private call to users not contained within the <entry> elements of the <PrivateCall> element;

   then:

   a) shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "144 user not authorised to call this particular user" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

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

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

11) shall set the Request-URI to the public service identity of the controlling MCPTT function hosting the private call service;

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

13) if the Priv-Answer-Mode header field specified in IETF RFC 5373 [18] was received in the incoming SIP INVITE request with a value of "Auto" or if no Priv-Answer-Mode header field was received in the incoming SIP INVITE request or a Priv-Answer-Mode header field was received containing a value other than "Auto", shall include the Priv-Answer-Mode header field set to a value of "Auto" in the outgoing SIP INVITE request;

14) shall include in the SIP INVITE request an SDP offer based on the SDP offer in the received "SIP INVITE request for originating participating MCPTT function", as specified in subclause 6.3.2.1.1.1; and

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

11.1.6.3.1.2 Receipt of SIP BYE request for on-demand ambient listening call

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

1) shall follow the procedures as specified in subclause 11.1.3.2.1.1.

11.1.6.3.1.3 Receipt of REFER "BYE" request for private call using pre-established session

Upon receiving from the MCPTT client a SIP REFER request when using a pre-established session with the "method" SIP URI parameter set to value "BYE" in the URI in the Refer-To header field the participating MCPTT function shall follow the procedures as specified in subclause 6.3.2.1.7.

11.1.6.3.1.4 Ambient listening call initiation using pre-established session

Upon receipt of a "SIP REFER request for a pre-established session", with:

1) the Refer-To header field containing a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 [62] that points to an application/resource-lists MIME body as specified in IETF RFC 5366 [20] containing one <entry> element with a "uri" attribute containing a SIP URI set to the MCPTT ID of the called user(s);

2) a "body" parameter of the SIP URI specified above containing an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element set to "ambient-listening"; and

3) a Content-ID header field set to the "cid" URL;

the participating 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;

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

3) if the participating MCPTT function cannot find a binding between the public user identity and an MCPTT ID or if the validity period of an existing binding has expired, then the participating MCPTT function shall reject the SIP REFER request with a SIP 404 (Not Found) response with the warning text set to "141 user unknown to the participating function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

4) if the received SIP REFER request does not contain an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field, shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

5) if the received SIP REFER request contains an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field with more than one <entry> element each with an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element, shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

6) if the received SIP REFER request contains an application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field with only one <entry> element with an application/vnd.3gpp.mcptt-info MIME body with the <session-type> element not set to "ambient-listening", shall reject the "SIP REFER request for pre-established session" with a SIP 403 (Forbidden) response including warning text set to "145 unable to determine called party" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

7) if the <ambient-listening-type> element of the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP REFER request is set to a value of:

   a) "remote-init" and an <allow-request-remote-initiated-ambient-listening> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false"; or

   b) "local-init" and an <allow-request-locally-initiated-ambient-listening> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) or is set to a value of "false";

   then shall reject the "SIP REFER request for a pre-established session" with a SIP 403 (Forbidden) response, with warning text set to "154 The MCPTT user is not authorised to make an ambient listening call" in a Warning header field as specified in subclause 4.4, and shall not continue with the rest of the steps;

8) shall determine the public service identity of the controlling MCPTT function for the ambient listening call service associated with the originating user's MCPTT ID;

NOTE 1: How the participating MCPTT server discovers the public service identity of the controlling MCPTT function associated with the ambient listening call service of the calling user is out of scope of the current document.

9) if the participating MCPTT function is unable to identify the controlling MCPTT function for the ambient listening call service associated with the originating user's MCPTT ID, it shall reject the REFER request with a SIP 404 (Not Found) response with the warning text "142 unable to determine the controlling function" in a Warning header field as specified in subclause 4.4, and shall not continue with any of the remaining steps;

10) if the <allow-private-call> element of the <ruleset> element is not present in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the participating MCPTT function or is present with the value "false", indicating that the user identified by the MCPTT ID is not authorised to initiate private calls, shall reject the "SIP REFER request for pre-established session"with a SIP 403 (Forbidden)

response to the SIP INVITE request, with warning text set to "107 user not authorised to make private calls" in a Warning header field as specified in subclause 4.4;

11) if the <PrivateCall> element exists in the MCPTT user profile document with one or more <entry> elements (see the MCPTT user profile document in 3GPP TS 24.484 [50]) and:

   a) the "uri" attribute of each and every <entry> element of the application/resource-lists MIME body referenced by a "cid" URL in the Refer-To header field does not match with any of the <entry> elements of the <PrivateCall> element of the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]); and

   b) if configuration is not set in the MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) that allows the MCPTT user to make a private call to users not contained within the <entry> elements of the <PrivateCall> element;

then:

   a) shall reject the "SIP INVITE request for originating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "144 user not authorised to call this particular user" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

12) if the "SIP REFER request for a pre-established session" contained a Refer-Sub header field containing "false" value and a Supported header field containing "norefersub" value, shall handle the SIP REFER request as specified in 3GPP TS 24.229 [4], IETF RFC 3515 [25] as updated by IETF RFC 6665 [26], and IETF RFC 4488 [22] without establishing an implicit subscription;

13) shall generate a final SIP 200 (OK) response to the "SIP REFER request for a pre-established session" according to 3GPP TS 24.229 [4];

NOTE 2: In accordance with IETF RFC 4488 [22], the participating MCPTT function inserts the Refer-Sub header field containing the value "false" in the SIP 200 (OK) response to the SIP REFER request to indicate that it has not created an implicit subscription.

14) shall include in the SIP 200 (OK) response the g.3gpp.mcptt.ambient-listening-call-release feature-capability indicator as described in clause D.3 in the Feature-Caps header field according to IETF RFC 6809 [60];

NOTE 3: The originator of the ambient listening call is either the initiator of a "remote-init" ambient listening type call or the originator of a "local-init" ambient listening type call. In either case, the originating user is allowed to release the ambient listening call.

15) shall send the response to the "SIP REFER request for a pre-established session" towards the MCPTT client according to 3GPP TS 24.229 [4];

16) shall generate a SIP INVITE request as specified in subclause 6.3.2.1.4;

17) shall include a Priv-Answer-Mode header field set to a value of "Auto" in the outgoing SIP INVITE request;

18) shall set the Request-URI of the SIP INVITE request to the public service identity of the controlling MCPTT function hosting the ambient listening call service for the calling MCPTT user as determined above in step 7); and

NOTE 4: The participating MCPTT function will leave verification of the Resource-Priority header field to the controlling MCPTT function.

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

Upon receiving SIP provisional responses for the SIP INVITE request the participating MCPTT function:

1) shall discard the received SIP responses without forwarding them.

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

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

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request in step 21) the participating MCPTT function:

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

11.1.6.3.2 Terminating procedures

11.1.6.3.2.1 Terminating procedures for ambient listening call

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

NOTE: The procedures in the present subclause are applicable for both on-demand and pre-established sessions.

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 for terminating participating MCPTT function" 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;

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) 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;

4) 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;

5) when the called user identified by the MCPTT ID is unable to participate in private calls as identified in the called user's MCPTT user profile document (see the MCPTT user profile document in 3GPP TS 24.484 [50]) on the terminating participating MCPTT function, shall reject the "SIP INVITE request for terminating participating MCPTT function" with a SIP 403 (Forbidden) response including warning text set to "127 user not authorised to be called in private call" in a Warning header field as specified in subclause 4.4; and

6) shall perform the automatic commencement procedures specified in subclause 6.3.2.2.5.1 and according to IETF RFC 5373 [18].

11.1.6.3.2.2 Receipt of SIP BYE request for on-demand ambient listening call

Upon receiving a SIP BYE request from the controlling MCPTT function, the participating MCPTT function shall follow the procedures as specified in subclause 11.1.3.2.2.1.

11.1.6.3.2.3 Receipt of SIP BYE request for an ongoing pre-established session

Upon receiving a SIP BYE request from the controlling MCPTT function for an ambient listening call and if the MCPTT session id refers to an MCPTT user that has a pre-established session with the participating MCPTT function, the participating MCPTT function:

1) if the SIP BYE request contains an application/vnd.3gpp.mcptt-info+xml MIME body:

   a) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [4] and IETF RFC 6086 [64];

   b) shall include the Info-Package header field set to g.3gpp.mcptt-info in the SIP INFO request;

   c) shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP BYE request to the SIP INFO request; and

   d) shall send the SIP INFO request towards the targeted MCPTT client in the dialog of the pre-established session according to 3GPP TS 24.229 [4].

Upon receiving a SIP 2xx response for the sent SIP INFO request, shall perform the procedures specified in subclause 11.1.3.2.2.2.

11.1.6.4 Controlling MCPTT function procedures

11.1.6.4.1 Originating procedures

This subclause describes the procedures for inviting an MCPTT user to an MCPTT ambient listening session. The procedure is initiated by the controlling MCPTT function as the result of an action in subclause 11.1.6.4.2

The controlling MCPTT function:

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

NOTE 1: As a result of calling subclause 6.3.3.1.2, the <mcptt-calling-user-id> containing the calling user's MCPTT ID is copied into the outgoing SIP INVITE.

2) shall copy the MCPTT ID of the MCPTT user listed in the MIME resources body of the incoming SIP INVITE request, into the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the outgoing SIP INVITE request;

3) 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 2: How the controlling MCPTT function finds the address of the terminating MCPTT participating function is out of the scope of the current release.

NOTE 3: 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.

4) shall copy the public user identity of the calling MCPTT user from the P-Asserted-Identity header field of the incoming SIP INVITE request into the P-Asserted-Identity header field of the SIP INVITE request;

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 <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP INVITE request is set to a value of "local-init", shall include the g.3gpp.mcptt.ambient-listening-call-release feature-capability indicator as described in clause D.3 in the Feature-Caps header field according to IETF RFC 6809 [60];

NOTE 4: The only case where the terminating user can release the ambient listening call is when the terminating client is the "listening MCPTT user";

7) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP INVITE request is set to a value of "remote-init", shall include in the outgoing SIP INVITE request an alert-info header field set to a value of "<file:///dev/null>" according to IETF RFC 3261 [24];

8) shall send the SIP INVITE request towards the core network according to 3GPP TS 24.229 [4]; and

9) shall start a private call timer with a value set to the configured max private call duration for the user.

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

1) shall cache the contact received in the Contact header field; and

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

Upon expiry of the private call timer, the controlling MCPTT function shall follow the procedure for releasing the ambient listening call session as specified in subclause 11.1.6.4.3 with the clarification that the <release-reason> element included in the SIP BYE request shall be set to "private-call-timer-expiry".

11.1.6.4.2 Terminating procedures

Upon receiving of a "SIP INVITE request for controlling MCPTT function of an ambient listening call" the controlling MCPTT function:

1) shall check whether the public service identity contained in the Request-URI is allocated for ambient listening call and perform the actions specified in subclause 6.3.7.1 if it is not allocated and skip the rest of the steps;

2) shall perform actions to verify the MCPTT ID of the inviting MCPTT user in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP INVITE request, and authorise the request according to local policy; and

3) if the request is not authorised as determined by step 2) above, the controlling MCPTT function shall return a SIP 403 (Forbidden) response with the warning text as specified in "Warning header field" and skip the rest of the steps;

4) shall validate that the received SDP offer includes at least one media stream for which the media parameters and at least one codec or media format is acceptable by the controlling MCPTT function and if not, reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

5) shall perform actions as described in subclause 6.3.3.2.2;

6) shall allocate an MCPTT session identity for the MCPTT ambient listening call session; and

7) shall invite the MCPTT user listed in the MIME resource-lists body of received SIP INVITE request as specified in subclause 11.1.6.4.1.

If the procedures of subclause 11.1.6.4.1 were successful in inviting the MCPTT user listed in the MIME resource-lists body of received SIP INVITE request, the controlling MCPTT function:

1) shall generate a SIP 200 (OK) response to the SIP INVITE request as specified in the subclause 6.3.3.2.3.2 before continuing with the rest of the steps;

2) 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 6.3.3.2.2;

3) shall include in the SIP 200 (OK) response the g.3gpp.mcptt.ambient-listening-call-release feature-capability indicator as described in clause D.3 in the Feature-Caps header field according to IETF RFC 6809 [60];

NOTE: The originator of the ambient listening call is either the initiator of a "remote-init" ambient listening type call or the originator of a "local-init" ambient listening type call. In either case, the originating user is allowed to release the ambient listening call.

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

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

6) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP INVITE request is set to a value of "remote-init":

   a) shall cache the MCPTT ID contained in the <mcptt-calling-user-id> element of the received SIP INVITE request as the listening MCPTT user of the ambient listening call and cache the MCPTT ID contained in the MIME resource-lists body of the received SIP INVITE request as the listened-to MCPTT user; and

   b) shall cache the ambient listening type of the ambient listening call as "remote-init"; and

7) if the <ambient-listening-type> element contained in the application/vnd.3gpp.mcptt-info+xml MIME body in the received SIP INVITE request is set to a value of "local-init":

   a) shall cache the MCPTT ID contained in the <mcptt-calling-user-id> element of the received SIP INVITE request as the listened-to MCPTT user of the ambient listening call and cache the MCPTT ID contained in the MIME resource-lists body of received SIP INVITE request as the listening MCPTT user; and

   b) shall cache the ambient listening type of the ambient listening call as "local-init".

If the procedures of subclause 11.1.6.4.1 were not successful in inviting the MCPTT user listed in the MIME resource-lists body of received SIP INVITE request, the controlling MCPTT function shall reject the received SIP INVITE request with a SIP 480 (Temporarily Unavailable) response and skip the remaining procedures of the present subclause.

The controlling MCPTT function shall forward any other SIP response that does not contain SDP, including any MIME bodies contained therein, along the signalling path to the originating network according to 3GPP TS 24.229 [4].

11.1.6.4.3 Server initiated ambient call release

The ambient listening call release is triggered by an MCPTT administrator by a mechanism outside of the scope of the standard, or directly by the controlling MCPTT function as a result of an event as specified in subclause 10.14.3.3 of 3GPP TS 23.379 [3].

This subclause is referenced from other procedures.

Upon receipt of a trigger to release an ongoing ambient listening call identified by the MCPTT ID of the listening MCPTT user, the MCPTT ID of the listened-to MCPTT user and the ambient listening type of the call, the controlling MCPTT function:

1) shall identify the MCPTT sessions of the listening MCPTT user and the MCPTT ID of the listened-to MCPTT user for the ambient listening call to be released;

2) shall interact with the media plane as specified in 3GPP TS 24.380 [5] for the MCPTT session release;

3) shall generate a SIP BYE request according to rules and procedures of 3GPP TS 24.229 [4] to be sent in the dialog for the ambient listening call with the MCPTT client of the listened-to MCPTT user; and

4) shall send the SIP BYE request in the dialog for the ambient listening call with the MCPTT client of the listened-to MCPTT user.

Upon receipt of a SIP 200 (OK) response to the SIP BYE request 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 requests according to 3GPP TS 24.229 [4];

3) shall include an application/vnd.3gpp.mcptt-info+xml MIME body in the SIP BYE request including a <release-reason> element set to a value of:

   a) "administrator-action" if triggered by an MCPTT administrator;

   b) "private-call-expiry" if the ambient listening call is released due to the expiry of the private call timer;

   c) "call-request-for-listened-to-client" if there is a call request targeted to the listened-to client; or

   d) "call-request-initiated-by-listened-to-client" if there is a call request initiated by the listened-to client; and

4) shall send the SIP BYE requests in the dialog for the ambient listening call with the MCPTT client of the listening MCPTT user according to3GPP TS 24.229 [4].

Upon receipt of a SIP 200 (OK) response to the SIP BYE request sent to MCPTT client of the listening MCPTT user the controlling MCPTT function:

1) shall delete the following cached data for the ambient listening call:

   a) the MCPTT ID of the listened-to MCPTT user

   b) the MCPTT ID of the listening MCPTT user; and

   c) the ambient listening type.

Upon receipt of a SIP 200 (OK) response to the 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 media plane resources associated with the SIP sessions with the MCPTT clients;

2) shall delete the following cached data for the ambient listening call:

   a) the MCPTT ID of the listened-to MCPTT user;

   b) the MCPTT ID of the listening MCPTT user; and

   c) the value of the ambient listening type.

11.1.6.4.4 Reception of a SIP BYE request

Upon receipt of a SIP BYE request for an ambient listening session 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;

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

3) shall send the SIP BYE request in the dialog of the other participant in the ambient listening call according to3GPP TS 24.229 [4];

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

5) shall send the SIP BYE request in the dialog of the participant in the ambient listening call according to3GPP TS 24.229 [4].

Upon receiving a SIP 200 (OK) response to the sent 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 media plane resources associated with the SIP session with the MCPTT ambient listening call participant;

2) shall generate a SIP 200 (OK) response to the received SIP BYE request and send the SIP 200 (OK) response towards the MCPTT client according to 3GPP TS 24.229 [4]; and

3) shall delete the following cached data for the ambient listening call:

   a) the MCPTT ID of the listened-to MCPTT user;

   b) the MCPTT ID of the listening MCPTT user; and

   c) the value of the ambient listening type.

11.2 Off-network private call

11.2.1 General

11.2.1.1 Common procedures

11.2.1.1.1 Sending/Receiving a message

In order to participate in a private call, the MCPTT client:

1) shall send the MONP message as a UDP message to the local IP address of the MCPTT user, on UDP port TBD, with an IP time-to-live set to 255; and

Editor's note [CT1#95, C1-160392]: Port number for the message is FFS.

2) shall treat UDP messages received on the port TBD as received MONP messages.

NOTE: An MCPTT client that supports IPv6 shall listen to the IPv6 addresses.

11.2.1.1.2 Session description

For an off-network MCPTT session, only MCPTT speech is used.

One off-network MCPTT session includes one media-floor control entity.

The MCPTT client shall generate an SDP body for a private call in accordance with rules and procedures of IETF RFC 4566 [12] and IETF RFC 3264 [44].

The MCPTT client:

1) shall include in the session-level section:

   a) the "o=" field with the <username> portion set to a dash;

   b) the "s=" field with the <session name> portion set to a dash; and

   c) the "c=" field with the <nettype> portion set to "IN", the <addrtype> portion set to the IP version of the unicast IP address of the MCPTT client and the <connection-address> portion set to the unicast IP address of the MCPTT client;

2) shall include the media-level section for MCPTT speech consisting of:

   a) the "m=" field with the <media> portion set to "audio", the <port> portion set to a port number for MCPTT speech of the MCPTT group, the <proto> field set to "RTP/AVP" and <fmt> portion set indicating RTP payload type numbers;

   b) the "i=" field with the <session description> portion set to "speech";

   c) the "a=fmtp:" attribute(s), the "a=rtpmap:" attribute(s) or both, indicating the codec(s) and media parameters of the MCPTT speech; and

   d) the "a=rtcp:" attribute indicating port number to be used for RTCP at the MCPTT client selected according to the rules and procedures of IETF RFC 3605 [13], if the media steam uses other than the default IP address;

3) shall include the media-level section for media-floor control entity consisting of:

   a) an "m=" line, with the <media> portion set to "application", the <port> portion set to a port number for media-floor control entity of the MCPTT group, the <proto> field set to "udp" and <fmt> portion set to "MCPTT"; and

   b) the "a=fmtp:MCPTT" attribute indicating the parameters of the media-floor control entity as specified 3GPP TS 24.380 [5]; and

4) shall include the MIKEY-SAKKE I_MESSAGE, if generated by the MCPTT client, in an "a=key-mgmt" attribute as a "mikey" attribute value in the SDP offer as specified in IETF RFC 4567 [47].

11.2.2 Basic call control

11.2.2.1 General

The maximum number of simultaneous off-network private calls is limited by the value of "/<*x*>/Common/PrivateCall/MaxCallN10" leaf node present in the UE configuration as specified in 3GPP TS 24.483 [45].

11.2.2.2 Private call control state machine

The figure 11.2.2.2-1 gives an overview of the main states and transitions on the UE for private call control.

Each private call control state machine is per MCPTT user ID.

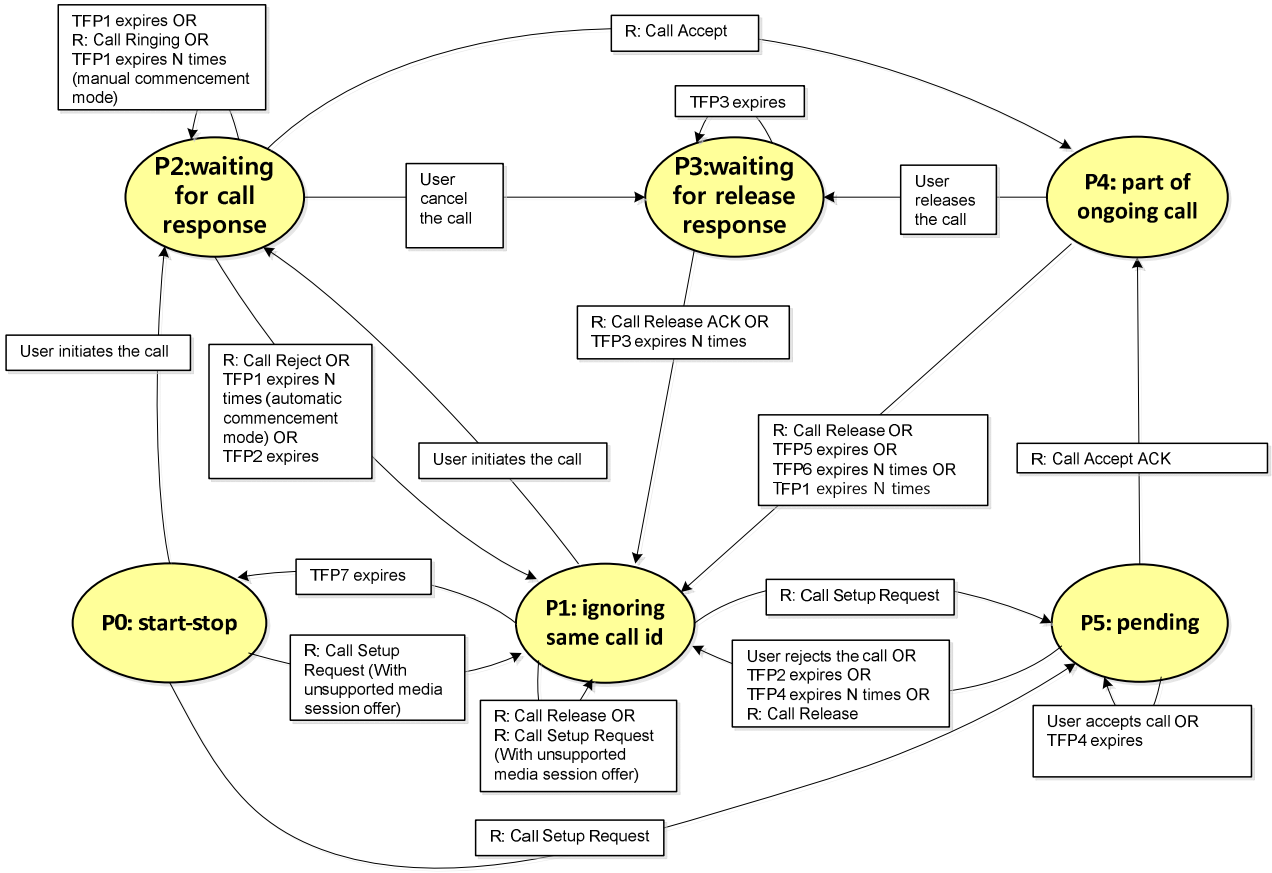

Figure 11.2.2.2-1: Private call control state machine

11.2.2.3 Private call control states

11.2.2.3.1 P0: start-stop

In this state, no private call control entity exists.

11.2.2.3.2 P1: ignoring same call id

This state exists for UE, when the UE is not part of an ongoing private call.

11.2.2.3.3 P2: waiting for call response

This state exists for UE, when the UE has sent a PRIVATE CALL SETUP REQUEST message and is waiting for a response, PRIVATE CALL ACCEPT or PRIVATE CALL REJECT message.

11.2.2.3.4 P3: waiting for release response

This state exists for UE, when the UE has sent a PRIVATE CALL RELEASE message and is waiting for a PRIVATE CALL RELEASE ACK message.

11.2.2.3.5 P4: part of ongoing call

This state exists for UE, when the UE is part of an ongoing private call.

11.2.2.3.6 P5: pending

This state exists for UE, when the UE has presented a notification to the user for the received PRIVATE CALL SETUP REQUEST message and is waiting for a user indication.

11.2.2.4 Procedures

11.2.2.4.1 General

11.2.2.4.2 Private call setup

11.2.2.4.2.1 Initiating a private call

When in the "P0: start-stop" state or "P1: ignoring same call id", upon an indication from MCPTT User to initiate a private call and the value of "/<x>/<x>/Common/PrivateCall/Authorised" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true", the MCPTT client:

1) shall generate and store the call identifier as a random number uniformly distributed between (0, 65536);

2) shall store own MCPTT user ID as caller ID;

3) shall store MCPTT user ID of the callee as callee ID;

4) shall store "AUTOMATIC COMMENCEMENT MODE" as commencement mode, if requested and the value of "/<x>/<x>/Common/PrivateCall/AutoCommence" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true". Otherwise if the value of "/<x>/<x>/Common/PrivateCall/ManualCommence" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true", store "MANUAL COMMENCEMENT MODE" as commencement mode;

5) shall create a call type control state machine as described in subclause 11.2.3.2;

6) if an end-to-end security context needs to be established then:

   a) shall use keying material provided by the key management server to generate a PCK as described in 3GPP TS 33.180 [78];

   b) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0001" to indicate that the purpose of the PCK is to protect private call communications and with the remaining twenty eight bits being randomly generated as described in 3GPP TS 33.180 [78];

   c) shall encrypt the PCK to a UID associated to the MCPTT client using the MCPTT ID and KMS URI of the invited user as determined by the procedures of subclause 6.2.8.3.9 and a time related parameter as described in 3GPP TS 33.180 [78];

   d) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [78];

   e) shall add the MCPTT ID of the originating MCPTT to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78];

   f) shall sign the MIKEY-SAKKE I_MESSAGE using the originating MCPTT user's signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.180 [78] and;

   g) shall store the MIKEY-SAKKE I_MESSAGE for later inclusion in an SDP body;

7) may store current user location as user location;

8) shall generate and store offer SDP, as defined in subclause 11.2.1.1.2;

9) shall generate a PRIVATE CALL SETUP REQUEST message as specified in subclause 15.1.5. In the PRIVATE CALL SETUP REQUEST message, the MCPTT client:

   a) shall set the Call identifier IE with the stored call identifier;

   b) shall set the MCPTT user ID of the caller IE with the stored caller ID;

   c) shall set the MCPTT user ID of the callee IE with the stored callee ID;

   d) shall set the Commencement mode IE with the stored commencement mode;

e) shall set the Call type IE with the stored current call type associated with the call type control state machine;

f) shall set the SDP offer IE with the stored offer SDP; and

g) may set the User location IE with the stored user location if the stored current call type associated with the call type control state machine is "EMERGENCY PRIVATE CALL".

10) shall send the PRIVATE CALL SETUP REQUEST message towards other MCPTT client according to rules and procedures as specified in subclause 11.2.1.1.1;

11) shall initialize the counter CFP1 (private call request retransmission) with the value set to 1;

12) shall start timer TFP1 (private call request retransmission); and

13) shall enter the "P2: waiting for call response" state.

11.2.2.4.2.2 Private call setup request retransmission

When in the "P2: waiting for call response" state, upon expiry of timer TFP1 (private call request retransmission), the MCPTT client:

1) may update the stored user location with current user location;

2) shall increment the value of counter CFP1 (private call request retransmission) by 1;

3) shall generate a PRIVATE CALL SETUP REQUEST message as specified in subclause 15.1.5. In the PRIVATE CALL SETUP REQUEST message, the MCPTT client:

a) shall set the Call identifier IE with the stored call identifier;

b) shall set the MCPTT user ID of the caller IE with the stored caller ID;

c) shall set the MCPTT user ID of the callee IE with the stored callee ID;

d) shall set the Commencement mode IE with the stored commencement mode;

e) shall set the Call type IE with the stored current call type associated with the call type control state machine;

f) shall set the SDP offer IE with the stored offer SDP; and

g) may set the User location IE with stored user location if the stored current call type is "EMERGENCY PRIVATE CALL" associated with the call type control state machine.

4) shall send the PRIVATE CALL SETUP REQUEST message towards other MCPTT client according to rules and procedures as specified in subclause 11.2.1.1.1;

5) shall start timer TFP1 (private call request retransmission); and

6) shall remain in the "P2: waiting for call response" state.

11.2.2.4.2.3 Ringing notification to the user

When in the "P2: waiting for call response" state, upon receiving a PRIVATE CALL RINGING message, the MCPTT client:

1) shall remain in the "P2: waiting for call response" state.

11.2.2.4.2.4 No response to private call setup request with automatic commencement mode

In the "P2: waiting for call response" state, when timer TFP1 (private call request retransmission) expires and the value of the counter CFP1 (private call request retransmission) is equal to the upper limit and the stored commencement mode is "AUTOMATIC COMMENCEMENT MODE", the MCPTT client:

1) shall start timer TFP7 (waiting for any message with same call identifier); and

2) shall enter the "P1: ignoring same call id" state.

11.2.2.4.2.5 No response to private call setup request with manual commencement mode

When in the "P2: waiting for call response" state when timer TFP1 (private call request retransmission) expires and the value of the counter CFP1 (private call request retransmission) is equal to the upper limit and the stored commencement mode is "MANUAL COMMENCEMENT MODE", the MCPTT client:

1) shall start timer TFP2 (waiting for call response message); and
2) shall remain in the "P2: waiting for call response" state.

11.2.2.4.2.6 No response to private call setup request after waiting for user acknowledgement

When in the "P2: waiting for call response" state, upon expiry of timer TFP2 (waiting for call response message), the MCPTT client:

1) shall start timer TFP7 (waiting for any message with same call identifier);
2) shall release the call control state machine; and
3) shall enter the "P1: ignoring same call id" state.

11.2.2.4.2.7 Private call setup request rejected

When in the "P2: waiting for call response" state, upon receiving a PRIVATE CALL REJECT message in response to PRIVATE CALL SETUP REQUEST message with Call identifier IE same as the stored call identifier, the MCPTT client:

1) shall stop timer TFP1 (call setup retransmission), if running;
2) shall stop timer TFP2 (waiting for call response message), if running;
3) shall start timer TFP7 (waiting for any message with same call identifier);
4) shall release the call control state machine; and
5) shall enter the "P1: ignoring same call id" state.

11.2.2.4.2.8 Private call setup request accepted

When in the "P2: waiting for call response" state, upon receiving a PRIVATE CALL ACCEPT message response to PRIVATE CALL SETUP REQUEST message with the same call identifier, the MCPTT client:

1) shall store the SDP answer IE received in the PRIVATE CALL ACCEPT message as answer SDP;
2) shall generate a PRIVATE CALL ACCEPT ACK message as specified in subclause 15.1.11:
   a) shall set the Call identifier IE to the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE with the stored caller ID; and
   c) shall set the MCPTT user ID of the callee IE with the stored callee ID.
3) shall send the PRIVATE CALL ACCEPT ACK message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;
4) shall stop timer TFP1 (call setup retransmission), if running;
5) shall stop timer TFP2 (waiting for call response message), if running;
6) shall establish a media session based on the SDP body of the stored answer SDP;
7) shall start floor control as terminating floor participant as specified in subclause 7.2 in 3GPP TS 24.380 [5];
8) shall start timer TFP5 (max duration); and
9) shall enter the "P4: part of ongoing call" state.

11.2.2.4.2.9 User cancels the private call setup request

When in the "P2: waiting for call response" state, upon an indication from MCPTT User to cancel the private call request, the MCPTT client:

1) shall generate a PRIVATE CALL RELEASE message as specified in subclause 15.1.9;
   a) shall set the Call identifier IE to the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE with the stored caller ID; and
   c) shall set the MCPTT user ID of the callee IE with the stored callee ID;
2) shall send the PRIVATE CALL RELEASE message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;
3) shall start timer TFP3 (private call release retransmission); and
4) shall enter the "P3: waiting for release response" state.

11.2.2.4.3 Private call setup in automatic commencement mode

11.2.2.4.3.1 Unable to establish media

When in the "P0: start-stop" or "P1: ignoring same call id" state, upon receiving a PRIVATE CALL SETUP REQUEST message with Call identifier IE different than stored call identifier and media session declared in SDP body of PRIVATE CALL SETUP REQUEST message cannot be established, the MCPTT client:

1) shall store the Call identifier IE in the received message as call identifier;
2) shall store the MCPTT user ID of the caller IE in the received PRIVATE CALL SETUP message as caller ID;
3) shall store own MCPTT user ID as callee ID;
4) shall generate a PRIVATE CALL REJECT message as specified in subclause 15.1.8. In the PRIVATE CALL REJECT message, the MCPTT client:
   a) shall set the Call identifier IE to the cached call identifier;
   b) shall set the MCPTT user ID of the caller IE with the stored caller ID;
   c) shall set the MCPTT user ID of the callee IE with stored callee ID; and
   d) shall set the Reason IE as "FAILED", if requested to restrict notification of call failure and the value of "/<x>/<x>/Common/PrivateCall/FailRestrict" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true". Otherwise, shall set the Reason IE as "MEDIA FAILURE".
5) shall send the PRIVATE CALL REJECT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;
6) shall start timer TFP7 (waiting for any message with same call identifier); and
7) shall enter the "P1: ignoring same call id" state if current state is the "P0: start-stop" state.

11.2.2.4.3.2 Responding to private call setup request when not participating in the ongoing call

When in the "P0: start-stop" or "P1: ignoring same call id" state, upon receiving a PRIVATE CALL SETUP REQUEST message with Commencement mode IE set to "AUTOMATIC COMMENCEMENT MODE" and Call identifier IE different than stored call identifier and media session declared in SDP body of PRIVATE CALL SETUP REQUEST message can be established, the MCPTT client:

1) shall store the Call identifier IE in the received message as call identifier;
2) shall create the call type control state machine as described in subclause 11.2.3.2;

3) shall store the MCPTT user ID of the caller IE in the received PRIVATE CALL SETUP REQUEST message as caller ID;

4) shall store own MCPTT user ID as callee ID;

5) if the SDP offer contains an "a=key-mgmt" attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

   a) shall extract the MCPTT ID of the originating MCPTT user from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78];

   b) shall convert the MCPTT ID to a UID as described in 3GPP TS 33.180 [78];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [78];

   d) if the validation of the signature failed, shall generate a PRIVATE CALL REJECT message as specified in subclause 15.1.8. In the PRIVATE CALL REJECT message, the MCPTT client:

      i) shall set the call identifier IE to the stored call identifier;

      ii) shall set the MCPTT user ID of the caller IE with the stored caller ID;

      iii) shall set the MCPTT user ID of the callee IE with the stored callee ID;

      iv) shall set the Reason IE as "FAILED", if requested to restrict notification of call failure and the value of "/<x>/<x>/Common/PrivateCall/FailRestrict" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true". Otherwise, shall set the reason IE as "E2E SECURITY CONTEXT FAILURE";

      v) shall send the PRIVATE CALL REJECT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1; and

      vi) shall remain in the current state;

   e) if the validation of the signature was successful:

      i) shall extract and decrypt the encapsulated PCK using the terminating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [78];

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [78];

      iii) shall generate and store answer SDP based on received SDP offer IE in PRIVATE CALL SETUP REQUEST message, as defined in subclause 11.2.1.1.2;

      iv) shall generate a PRIVATE CALL ACCEPT message as specified in subclause 15.1.7. In the PRIVATE CALL ACCEPT message, the MCPTT client:

         A) shall set the Call identifier IE to the stored call identifier; and

         B) shall set the MCPTT user ID of the caller IE with stored caller ID.

         C) shall set the MCPTT user ID of the callee IE with stored callee ID; and

         D) shall set the SDP answer IE with the stored answer SDP;

      v) shall send PRIVATE CALL ACCEPT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

      vi) shall establish a media session based on the SDP body of the stored answer SDP;

      vii) shall initialize the counter CFP4 with value set to 1;

      viii) shall start timer TFP4 (private call accept retransmission); and

      ix) shall enter the "P5: pending" state; and

NOTE: With the PCK successfully shared between the originating MCPTT client and the terminating MCPTT client, both clients are able to use SRTP/SRTCP to create an end-to-end secure session.

6) if the SDP offer does not contain an "a=key-mgmt" attribute, the MCPTT client:

   a) shall generate and store answer SDP based on received SDP offer IE in PRIVATE CALL SETUP REQUEST message, as defined in subclause 11.2.1.1.2;

   b) shall generate a PRIVATE CALL ACCEPT message as specified in subclause 15.1.7:

      i) shall set the Call identifier IE to the stored call identifier;

      ii) shall set the MCPTT user ID of the caller IE with stored caller ID.

      iii) shall set the MCPTT user ID of the callee IE with stored callee ID; and

      iv) shall set the SDP answer IE with the stored answer SDP;

   c) shall send PRIVATE CALL ACCEPT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

   d) shall establish a media session based on the SDP body of the stored answer SDP;

   e) shall initialize the counter CFP4 with value set to 1;

   f) shall start timer TFP4 (private call accept retransmission); and

   g) shall enter the "P5: pending" state.

11.2.2.4.3.3 Private call accept retransmission

When in the "P5: pending" state, upon expiry of timer TFP4 (private call accept retransmission), the MCPTT client:

1) shall generate a PRIVATE CALL ACCEPT message as specified in subclause 15.1.7. In the PRIVATE CALL ACCEPT message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier;

   b) shall set the MCPTT user ID of the caller IE with the stored caller ID;

   c) shall set the MCPTT user ID of the callee IE with the stored callee ID; and

   d) shall set the SDP answer IE with the stored answer SDP;

2) shall send PRIVATE CALL ACCEPT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

3) shall increment the value of the counter CFP4 (private call accept retransmission) by 1;

4) shall start timer TFP4 (private call accept retransmission); and

5) shall remain in the "P5: pending" state.

11.2.2.4.3.4 Establishing the call

When in the "P5: pending" state, upon receiving a PRIVATE CALL ACCEPT ACK message or RTP media from originating user, the MCPTT client:

1) shall stop timer TFP4(private call accept retransmission);

2) shall start floor control as terminating MCPTT client as specified in subclause 7.2 in 3GPP TS 24.380 [5];

3) shall start timer TFP5 (max duration); and

4) shall enter the "P4: part of ongoing call" state.

11.2.2.4.3.5 Call failure

In the "P5: pending" state, when timer TFP4 (private call accept retransmission) expires and the value of the counter CFP4 (private call accept retransmission) is equal to the upper limit, the MCPTT client:

1) shall start timer TFP7 (waiting for any message with same call identifier);
2) shall release the call type control state machine; and
3) shall enter the "P1: ignoring same call id" state.

11.2.2.4.4 Private call setup in manual commencement mode

11.2.2.4.4.1 Incoming private call

When in the "P0: start-stop" or "P1: ignoring same call id" state, upon receiving a PRIVATE CALL SETUP REQUEST message with Commencement mode IE set to "MANUAL COMMENCEMENT MODE" and Call identifier IE different from stored call identifier, the MCPTT client:

1) shall store the Call identifier IE in the received message as call identifier;
2) shall create the call type control state machine as described in subclause 11.2.3.2;
3) shall store the MCPTT user ID of the caller IE as received in the PRIVATE CALL SETUP REQUEST as caller ID;
4) shall store own MCPTT user ID as callee ID;
5) shall generate a PRIVATE CALL RINGING message as specified in subclause 15.1.6;
   a) shall set the Call identifier IE to the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE with the stored caller ID; and
   c) shall set the MCPTT user ID of the callee IE with the stored callee ID;
6) shall send PRIVATE CALL RINGING message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;
7) shall start timer TFP2 (waiting for call response message); and
8) shall enter the "P5: pending" state.

11.2.2.4.4.2 No response from the user

When in the "P5: pending" state, upon expiry of timer TFP2 (waiting for call response message), the MCPTT client:

1) shall generate a PRIVATE CALL REJECT message as specified in subclause 15.1.8:
   a) shall set the Call identifier IE to the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE with the stored caller ID;
   c) shall set the MCPTT user ID of the callee IE with the stored callee ID; and
   d) shall set the Reason IE as "FAILED".
2) shall send the PRIVATE CALL REJECT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;
3) shall start timer TFP7 (waiting for any message with same call identifier);
4) shall release the call type control state machine; and

5) shall enter the "P1: ignoring same call id" state.

11.2.2.4.4.3 User accepts the private call setup request

When in the "P5: pending" state, upon an indication from MCPTT User to accept the incoming private call, the MCPTT client:

1) if the SDP offer contains an "a=key-mgmt" attribute field with a "mikey" attribute value containing a MIKEY-SAKKE I_MESSAGE:

   a) shall extract the MCPTT ID of the originating MCPTT user from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78];

   b) shall convert the MCPTT ID to a UID as described in 3GPP TS 33.180 [78];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [78];

   d) if the validation of the signature failed, shall generate a PRIVATE CALL REJECT message as specified in subclause 15.1.8. In the PRIVATE CALL REJECT message, the MCPTT client:

      i) shall set the call identifier IE to the stored call identifier;

      ii) shall set the MCPTT user ID of the caller IE with the stored caller ID;

      iii) shall set the MCPTT user ID of the callee IE with the stored callee ID;

      iv) shall set the Reason IE as "FAILED", if requested to restrict notification of call failure and the value of "/<x>/<x>/Common/PrivateCall/FailRestrict" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true". Otherwise, shall set the reason IE as "E2E SECURITY CONTEXT FAILURE";

      v) shall send the PRIVATE CALL REJECT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1; and

      vi) shall enter the "P1: ignoring same call id" state;

   e) if the validation of the signature was successful:

      i) shall extract and decrypt the encapsulated PCK using the terminating user's (KMS provisioned) UID key as described in 3GPP TS 33.180 [78];

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [78];

      iii) shall generate and store answer SDP based on received SDP offer IE in PRIVATE CALL SETUP REQUEST message, as defined in subclause 11.2.1.1.2;

      iv) shall generate a PRIVATE CALL ACCEPT message as specified in subclause 15.1.7. In the PRIVATE CALL ACCEPT message, the MCPTT client:

         A) shall set the Call identifier IE to the stored call identifier;

         B) shall set the MCPTT user ID of the caller IE with the stored caller ID;

         C) shall set the MCPTT user ID of the callee IE with the stored callee ID; and

         D) shall set the SDP answer IE with the stored answer SDP;

      v) shall send the PRIVATE CALL ACCEPT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

      vi) shall establish a media session based on the SDP body of the private call;

      vii) shall stop timer TFP2 (waiting for call response message);

      viii) shall initialize the counter CFP4 with value set to 1;

ix) shall start timer TFP4 (private call accept retransmission); and

x) shall remain in the "P5: pending" state; and

NOTE: With the PCK successfully shared between the originating MCPTT client and the terminating MCPTT client, both clients are able to use SRTP/SRTCP to create an end-to-end secure session.

2) if the SDP offer does not contain an "a=key-mgmt" attribute, the MCPTT client:

a) shall generate and store answer SDP based on received SDP offer IE in PRIVATE CALL SETUP REQUEST message, as defined in subclause 11.2.1.1.2;

b) shall generate a PRIVATE CALL ACCEPT message as specified in subclause 15.1.7. In the PRIVATE CALL ACCEPT message, the MCPTT client:

i) shall set the Call identifier IE to the stored call identifier;

ii) shall set the MCPTT user ID of the caller IE with the stored caller ID;

iii) shall set the MCPTT user ID of the callee IE with the stored callee ID; and

iv) shall set the SDP answer IE with the stored answer SDP;

c) shall send the PRIVATE CALL ACCEPT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

d) shall establish a media session based on the SDP body of the private call;

e) shall stop timer TFP2 (waiting for call response message);

f) shall initialize the counter CFP4 with value set to 1;

g) shall start timer TFP4 (private call accept retransmission); and

h) shall remain in the "P5: pending" state.

11.2.2.4.4.4 Private call accept retransmission

When in the "P5: pending" state, upon expiry of timer TFP4 (private call accept retransmission), the MCPTT client:

1) shall generate a PRIVATE CALL ACCEPT message as specified in subclause 15.1.7. In the PRIVATE CALL ACCEPT message, the MCPTT client:

a) shall set the Call identifier IE to the stored call identifier;

b) shall set the MCPTT user ID of the caller IE the stored caller ID;

c) shall set the MCPTT user ID of the callee IE with the stored callee ID; and

d) shall set the SDP answer IE with the stored answer SDP;

2) shall send PRIVATE CALL ACCEPT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

3) shall increment the value of the (counter CFP4 private call accept retransmission) by 1;

4) shall start timer TFP4 (private call accept retransmission); and

5) shall remain in the "P5: pending" state.

11.2.2.4.4.5 Establishing the call

When in the "P5: pending" state, upon receiving a PRIVATE CALL ACCEPT ACK message or RTP media from originating user, the MCPTT client:

1) shall stop timer TFP4 (private call accept retransmission);

2) shall start floor control as terminating MCPTT client as specified in subclause 7.2 in 3GPP TS 24.380 [5];

3) shall start timer TFP5 (max duration); and

4) shall enter the "P4: part of ongoing call" state.

11.2.2.4.4.6 Call failure

In the "P5: pending" state, when timer TFP4 (private call accept retransmission) expires and the value of the counter CFP4 (private call accept retransmission) is equal to the upper limit, the MCPTT client:

1) shall start timer TFP7 (waiting for any message with same call identifier);

2) shall release the call type control state machine; and

3) shall enter the "P1: ignoring same call id" state.

11.2.2.4.4.7 User rejects the private call setup request

When in the "P5: pending" state, upon an indication from MCPTT User to reject the incoming private call, the MCPTT client:

1) shall generate a PRIVATE CALL REJECT message as specified in subclause 15.1.8:

   a) shall set the Call identifier IE to the stored call identifier;

   b) shall set the MCPTT user ID of the caller IE with the stored caller ID;

   c) shall set the MCPTT user ID of the callee IE with stored callee ID; and

   d) shall set the Reason IE as "FAILED", if requested to restrict notification of call failure and the value of "/<x>/<x>/Common/PrivateCall/FailRestrict" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true". Otherwise, shall set the Reason IE as "REJECT";

2) shall send the PRIVATE CALL REJECT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

3) shall start timer TFP7 (waiting for any message with same call identifier);

4) shall release the call type control state machine; and

5) shall enter the "P1: ignoring same call id" state.

11.2.2.4.4.8 Caller cancels the private call setup request before call establishment

When in the "P5: pending" state or "P1: ignoring same call id" state, upon receiving a PRIVATE CALL RELEASE message, the MCPTT client:

1) shall generate a PRIVATE CALL RELEASE ACK message as specified in subclause 15.1.10. In the PRIVATE CALL RELEASE ACK message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier;

   b) shall set the MCPTT user ID of the caller IE with the stored caller ID; and.

   c) shall set the MCPTT user ID of the callee IE with the stored callee ID.

2) shall send the PRIVATE CALL RELEASE ACK message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

3) shall start timer TFP7 (waiting for any message with same call identifier);

4) shall stop timer TFP4 (private call accept retransmission) if running;

5) shall release the call type control state machine, if the current state is "P5: pending" state; and

6) shall enter the "P1: ignoring same call id" state, if the current state is "P5: pending" state.

11.2.2.4.5 Private call release

11.2.2.4.5.1 Releasing a private call

When in the "P4: part of ongoing call" state, upon an indication from MCPTT User to release a private call, the MCPTT client:

1) shall generate a PRIVATE CALL RELEASE message as specified in subclause 15.1.9. In the PRIVATE CALL RELEASE message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier;

   b) shall set the MCPTT user ID of the caller IE with stored caller ID; and

   c) shall set the MCPTT user ID of the callee IE with stored callee ID.

2) shall send the PRIVATE CALL RELEASE message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

3) shall initialize the counter CFP3 (private call release retransmission) with the value set to 1;

4) shall start timer TFP3 (private call release retransmission); and

5) shall enter the "P3: waiting for release response" state.

11.2.2.4.5.2 Private call release retransmission

When in the "P3: waiting for release response" state, upon expiry of timer TFP3 (private call release retransmission), the MCPTT client:

1) shall generate a PRIVATE CALL RELEASE message as specified in subclause 15.1.9. In the PRIVATE CALL RELEASE message, the MCPTT client:

   a) shall set the Call identifier IE to the stored call identifier;

   b) shall set the MCPTT user ID of the caller IE with stored caller ID; and

   c) shall set the MCPTT user ID of the callee IE with the stored callee ID.

2) shall send the PRIVATE CALL RELEASE message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

3) shall increment the value of timer CFP3 by 1;

4) shall start timer TFP3 (private call release retransmission); and

5) shall remain in the "P3: waiting for release response" state.

11.2.2.4.5.3 No response to private call release

In the "P3: waiting for release response" state, when timer TFP3 (private call request retransmission) expires and the value of the counter CFP3 (private call release retransmission) is equal to the upper limit, the MCPTT client:

1) shall terminate the media session;

2) shall start timer TFP7 (waiting for any message with same call identifier);

3) shall release the call type control state machine; and

4) shall enter the "P1: ignoring same call id" state.

11.2.2.4.5.4 Acknowledging private call release after call establishment

When in the "P4: part of ongoing call" state, upon receiving a PRIVATE CALL RELEASE message, the MCPTT client:

1) shall generate a PRIVATE CALL RELEASE ACK message as specified in subclause 15.1.10;
   a) shall set the Call identifier IE to the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE the stored caller ID; and
   c) shall set the MCPTT user ID of the callee IE with the stored callee ID.
2) shall send the PRIVATE CALL RELEASE ACK message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;
3) shall terminate the media session for private call;
4) shall start timer TFP7 (waiting for any message with same call identifier);
5) shall release the call type control state machine; and
6) shall enter the "P1: ignoring same call id" state.

11.2.2.4.5.5 Private call release acknowledged

When in the "P3: waiting for release response" state, upon receiving a PRIVATE CALL RELEASE ACK to PRIVATE CALL RELEASE message, the MCPTT client:

1) shall stop timer TFP3 (private call release retransmission), if running;
2) shall terminate the media session;
3) shall start timer TFP7 (waiting for any message with same call identifier);
4) shall release the call type control state machine; and
5) shall enter the "P1: ignoring same call id" state.

11.2.2.4.5.6 Max duration reached

When in the "P4: part of ongoing call" state, upon expiry of timer TFP5 (max duration), the MCPTT client:

1) shall terminate the media session;
2) shall start timer TFP7 (waiting for any message with same call identifier);
3) shall release the call type control state machine; and
4) shall enter the "P1: ignoring same call id" state.

11.2.2.4.5.7 Stop ignoring same call id

When in the "P1: ignoring same call id" state, upon expiry of timer TFP7 (waiting for any message with same call identifier) the MCPTT client:

1) shall clear the stored call identifier; and
2) shall enter the "P0: start-stop" state.

11.2.2.4.5.8 No response to emergency private call setup request

In the "P4: part of ongoing call" state, when timer TFP1 (private call request retransmission) expires and the value of the counter CFP1 (private call request retransmission) is equal to the upper limit, the MCPTT client:

1) shall start timer TFP7 (waiting for any message with same call identifier);

2) shall release the call type control state machine; and

3) shall enter the "P1: ignoring same call id" state.

11.2.2.4.5.9 No response to emergency private call cancel

In the "P4: part of ongoing call" state, when timer TFP6 (emergency private call cancel retransmission) expires and the value of the counter CFP6 (emergency private call cancel retransmission) is equal to the upper limit, the MCPTT client:

1) shall start timer TFP7 (waiting for any message with same call identifier);

2) shall release the call type control state machine; and

3) shall enter the "P1: ignoring same call id" state.

11.2.2.4.6 Error handling

11.2.2.4.6.1 Unexpected MONP message received

Upon receiving a MONP message in a state where there is no handling specified for the MONP message, the MCPTT client shall discard the MONP message.

11.2.2.4.6.2 Unexpected indication from MCPTT user

Upon receiving an indication from the MCPTT user in a state where there is no handling specified for the indication, the MCPTT client shall ignore the indication.

11.2.2.4.6.3 Unexpected expiration of a timer

Upon expiration of a timer in a state where there is no handling specified for expiration of the timer, the MCPTT client shall ignore the expiration of the timer.

11.2.3 Call type control

11.2.3.1 General

This state machine exists in parallel with the call type control state machine for off-network private call as specified in subclause 11.2.2.2.

11.2.3.2 Call type control state machine

The Figure 11.2.3.2-1 gives an overview of the states and transitions of the state machine.

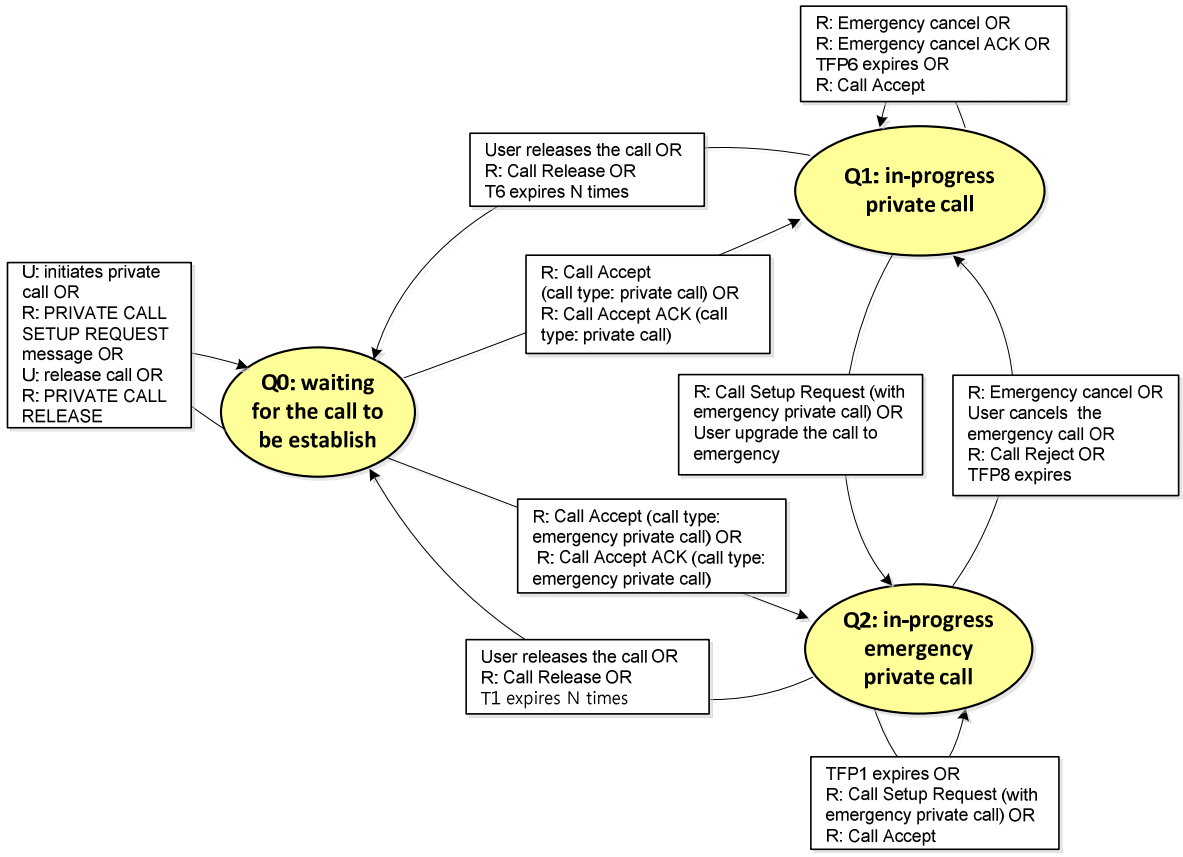

Figure 11.2.3.2-1: Call type state machine

When sending the message, MCPTT client indicates the stored current ProSe per-packet priority associated with the call type control state machine to the lower layers.

11.2.3.3 Call type control states

11.2.3.3.1 Q0: waiting for the call to be established

This state is the start state of this state machine.

11.2.3.3.2 Q1: in-progress private call

This state exists for UE, when the UE is part of an in-progress private call.

11.2.3.3.3 Q2: in-progress emergency private call

This state exists for UE, when the UE is part of an in-progress emergency private call.

11.2.3.4 Procedures

11.2.3.4.1 General

11.2.3.4.2 Outgoing call initiated

When in "Q0: waiting for the call to be established" state, upon an indication from the MCPTT user to initiate a call, the MCPTT client:

1) if the stored emergency state associated with emergency alert state machine described in 12.2.2.2 is set to "true" and the value of "/<*x*>/<*x*>/Common/PrivateCall/EmergencyCall/Authorised" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true":

   a) shall set the stored current call type to "EMERGENCY PRIVATE CALL"; and

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency private call as described in 3GPP TS 24.483 [45]; or

2) if the stored emergency state associated with emergency alert state machine described in 12.2.2.2 is set to "false":

   a) if the user initiates an MCPTT emergency private call and the value of "/<*x*>/<*x*>/Common/PrivateCall/EmergencyCall/Authorised" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true":

      i) shall set the stored current call type to "EMERGENCY PRIVATE CALL"; and

      ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency private call as described in 3GPP TS 24.483 [45]; or

   b) if the user initiates an MCPTT private call:

      i) shall set the stored current call type to "PRIVATE CALL"; and

      ii) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network private call as described in 3GPP TS 24.483 [45].

11.2.3.4.3 Received incoming call

When in "Q0: waiting for the call to be established" state, upon receipt of a PRIVATE CALL SETUP REQUEST message by an idle MCPTT client, the MCPTT client:

1) if the Call type IE of the received PRIVATE CALL SETUP REQUEST message is set to "EMERGENCY PRIVATE CALL":

   a) shall set the stored current call type to "EMERGENCY PRIVATE CALL"; and

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network emergency private call as described in 3GPP TS 24.483 [45];

2) if the Call type IE of the received PRIVATE CALL SETUP REQUEST message is set to "PRIVATE CALL":

   a) shall set the stored current call type to "PRIVATE CALL"; and

   b) shall set the stored current ProSe per-packet priority to value corresponding to MCPTT off-network private call as described in 3GPP TS 24.483 [45].

11.2.3.4.4 Establishing the private call

When in "Q0: waiting for the call to be established" state, upon receiving PRIVATE CALL ACCEPT message or PRIVATE CALL ACCEPT ACK message, the MCPTT client:

1) if the stored current call type is set to "EMERGENCY PRIVATE CALL":

   a) shall start TFP8 (implicit downgrade) timer; and

   b) shall enter "Q2: in-progress emergency private call" state; or

2) if the stored current call type is set to "PRIVATE CALL":

   a) shall enter "Q1: in-progress private call" state.

11.2.3.4.5 Upgrade call

11.2.3.4.5.1 User upgrades private call to emergency private call

When in the "Q1: in-progress private call" state, upon an indication from MCPTT User to upgrade the call to emergency and the value of "/<*x*>/<*x*>/Common/PrivateCall/EmergencyCall/Authorised" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true", the MCPTT client:

1) shall generate and store emergency offer SDP as defined in subclause 11.2.1.1.2;
2) shall update caller ID as own MCPTT user ID;
3) shall update callee ID as MCPTT user ID of the other user;
4) shall store current user location as user location;
5) shall set the stored current call type to "EMERGENCY PRIVATE CALL";
6) shall generate a PRIVATE CALL SETUP REQUEST message as specified in subclause 15.1.5. In the PRIVATE SETUP REQUEST message, the MCPTT client:
   a) shall set the Call identifier IE with the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE with stored caller ID;
   c) shall set the MCPTT user ID of the callee IE with the stored callee ID;
   d) shall set the Commencement mode IE as "AUTOMATIC COMMENCEMENT MODE";
   e) shall set the Call type IE to the stored current call type;
   f) shall set the SDP offer IE with emergency offer SDP; and
   g) may set the User location IE with user location.
7) shall set the ProSe per-packet priority to the value corresponding to MCPTT off-network emergency private call as described in 3GPP TS 24.483 [45];
8) shall send the PRIVATE CALL SETUP REQUEST message towards other MCPTT client according to rules and procedures as specified in subclause 11.2.1.1.1;
9) shall initialize the counter CFP1 (private call request retransmission) with value set to 1;
10) shall start timer TFP1 (private call request retransmission); and
11) shall enter the "Q2: in-progress emergency private call" state.

11.2.3.4.5.2 Emergency private call setup request retransmission

When in the "Q2: in-progress emergency private call" state, upon expiry of timer TFP1 (private call request retransmission), the MCPTT client:

1) may update the stored user location with current user location;
2) shall increment the value of the counter CFP1 (private call request retransmission) by 1;
3) shall generate a PRIVATE CALL SETUP REQUEST message as specified in subclause 15.1.5. In the PRIVATE CALL SETUP REQUEST message, the MCPTT client:
   a) shall set the Call identifier IE with the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE with stored caller ID;
   c) shall set the MCPTT user ID of the callee IE with stored callee ID;
   d) shall set the Commencement mode IE as "AUTOMATIC COMMENCEMENT MODE";

e) shall set the Call type IE to the stored current call type;

f) shall set the SDP offer IE with the stored emergency offer SDP; and

g) may set the User location IE with stored user location;

4) shall send the PRIVATE CALL SETUP REQUEST message towards other MCPTT client according to rules and procedures as specified in subclause 11.2.1.1.1;

5) shall start timer TFP1 (private call request retransmission); and

6) shall remain in the "Q2: in-progress emergency private call" state.

11.2.3.4.5.3 Emergency private call setup request accepted

When in the "Q2: in-progress emergency private call" state or in the "Q1: in-progress private call" state, upon receiving a PRIVATE CALL ACCEPT message response to PRIVATE CALL SETUP REQUEST message with the same call identifier, the MCPTT client:

1) shall store the SDP answer IE received in the PRIVATE CALL ACCEPT message as emergency answer SDP;

2) shall generate a PRIVATE CALL ACCEPT ACK message as specified in subclause 15.1.11:

a) shall set the Call identifier IE to the stored call identifier;

b) shall set the MCPTT user ID of the caller IE with stored caller ID; and

c) shall set the MCPTT user ID of the callee IE with the stored callee ID;

3) shall send the PRIVATE CALL ACCEPT ACK message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

4) shall stop timer TFP1 (call setup retransmission), if running;

5) shall stop timer TFP2 (waiting for call response message) , if running;

6) shall start TFP8 (implicit downgrade) timer;

7) shall establish a media session based on the SDP body of the stored emergency answer SDP; and

8) shall remain in the current state.

NOTE: PRIVATE CALL ACCEPT ACK message is retransmitted as described in this subclause, every time a PRIVATE CALL ACCEPT message is received.

11.2.3.4.5.4 Emergency private call setup request rejected

When in the "Q2: in-progress emergency private call" state, upon receiving a PRIVATE CALL REJECT message in response to PRIVATE CALL SETUP REQUEST message with Call identifier IE same as stored call identifier, the MCPTT client:

1) shall stop timer TFP1 (call setup retransmission), if running;

2) shall set the ProSe per-packet priority to the value corresponding to the MCPTT off-network private call as described in 3GPP TS 24.483 [45];

3) shall set the stored current call type to "PRIVATE CALL"; and

4) shall enter the "Q1: in-progress private call" state.

11.2.3.4.5.5 No response to emergency private call setup request

In the "Q2: in-progress emergency private call" state, when timer TFP1 (private call request retransmission) expires and the value of the counter CFP1 (private call request retransmission) is equal to the upper, the MCPTT client:

1) shall release the stored current call type;

2) shall release the stored Prose per-packet priority; and

3) shall enter "Q0: waiting for the call to be established".

11.2.3.4.5.6 Responding to emergency private call setup request when participating in the ongoing call

When in the "Q1: in-progress private call" state or "Q2: in-progress emergency private call" state, upon receiving a PRIVATE CALL SETUP REQUEST message with the Call identifier IE same as the stored call identifier of the call, the Call type IE set as "EMERGENCY PRIVATE CALL", the MCPTT client:

1) if the media session declared in SDP body of PRIVATE CALL SETUP REQUEST message can be established:

   a) shall generate and store emergency answer SDP based on received SDP offer IE in PRIVATE CALL SETUP REQUEST message, as defined in subclause 11.2.1.1.2;

   b) shall update the caller ID with the MCPTT user ID of the caller IE as received in the PRIVATE CALL SETUP REQUEST message;

   c) shall update the callee ID with own MCPTT user ID;

   d) shall generate a PRIVATE CALL ACCEPT message as specified in subclause 15.1.7:

      i) shall set the Call identifier IE to the stored call identifier;

      ii) shall set the MCPTT user ID of the callee IE with stored callee ID;

      iii) shall set the MCPTT user ID of the caller IE with stored caller ID; and

      iv) shall set the SDP answer IE with the stored emergency answer SDP;

   e) shall set the ProSe per-packet priority to the value corresponding to MCPTT off-network emergency private call as described in 3GPP TS 24.483 [45];

   f) shall start TFP8 (implicit downgrade) timer;

   g) shall send PRIVATE CALL ACCEPT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1;

   h) shall set the stored current call type to "EMERGENCY PRIVATE CALL"; and

   i) shall enter the "Q2: in-progress emergency private call" state;

2) if the media session declared in SDP body of PRIVATE CALL SETUP REQUEST message cannot be established:

   a) shall generate a PRIVATE CALL REJECT message as specified in subclause 15.1.8;

   b) shall set the call identifier IE with the call identifier in the received message;

   c) shall set the MCPTT user ID of the caller IE with the caller ID in the received message;

   d) shall set the MCPTT user ID of the callee IE with the callee ID in the received message;

   e) shall set the Reason IE as "FAILED", if requested to restrict notification of call failure and the value of "/<x>/<x>/Common/PrivateCall/FailRestrict" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] is set to "true". Otherwise, shall set the reason IE as "MEDIA FAILURE";

   f) shall send a PRIVATE CALL REJECT message in response to the request message according to rules and procedures as specified in subclause 11.2.1.1.1; and

   g) shall remain in the current state.

11.2.3.4.6 Downgrade call

11.2.3.4.6.1 User cancels the emergency private call

When in the "Q2: in-progress emergency private call" state, upon an indication from:

1) the caller of the emergency private call; or
2) the recipient of the emergency private call with the value of "/<*x*>/<*x*>/Common/PrivateCall/EmergencyCall/CancelPriority" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] set to "true",

to cancel the emergency private call, the MCPTT client:

1) shall generate a PRIVATE CALL EMERGENCY CANCEL message as specified in subclause 15.1.12. In the PRIVATE CALL EMERGENCY CANCEL message, the MCPTT client:
   a) shall set the Call identifier IE to the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE with the stored caller; and
   c) shall set the MCPTT user ID of the callee IE with the stored callee.
2) shall send the PRIVATE CALL EMERGENCY CANCEL message according to rules and procedures as specified in subclause 11.2.1.1.1;
3) shall stop TFP8 (implicit downgrade) timer;
4) shall initialize the counter CFP6 (emergency private call cancel retransmission) with the value set to 1;
5) shall start timer TFP6 (emergency private call cancel retransmission);
6) shall set the stored current call type to "PRIVATE CALL"; and
7) shall enter the "Q1: in-progress private call" state.

11.2.3.4.6.2 Emergency private call cancel retransmission

When in the "Q1: in-progress private call" state, upon expiry of timer TFP6 (emergency private call cancel retransmission), the MCPTT client:

1) shall generate a PRIVATE CALL EMERGENCY CANCEL message as specified in subclause 15.1.12. In the PRIVATE CALL EMERGENCY CANCEL message, the MCPTT client:
   a) shall set the Call identifier IE to the stored call identifier;
   b) shall set the MCPTT user ID of the caller IE with the stored caller ID; and
   c) shall set the MCPTT user ID of the callee IE with store callee ID.
2) shall send the PRIVATE CALL EMERGENCY CANCEL message according to rules and procedures as specified in subclause 11.2.1.1.1;
3) shall increment the value of the timer CFP6 (emergency private call cancel retransmission) by 1;
4) shall start timer TFP6 (emergency private call cancel retransmission); and
5) shall remain in the "Q1: in-progress private call" state.

11.2.3.4.6.3 Emergency private call cancel accepted

When in the "Q1: in-progress private call" state, upon receiving a PRIVATE CALL EMERGENCY CANCEL ACK message response to PRIVATE CALL EMERGENCY CANCEL message with the same "call identifier", the MCPTT client:

1) shall stop timer TFP6 (emergency private call cancel retransmission), if running;

2) shall establish a media session based on the SDP body of the stored answer SDP;

3) shall set the ProSe per-packet priority to the value corresponding to MCPTT off-network private call as described in 3GPP TS 24.483 [45]; and

4) shall remain in the "Q1: in-progress private call" state.

11.2.3.4.6.4 No response to emergency private call cancel

In the "Q1: in-progress private call" state, when timer TFP6 (emergency private call cancel retransmission) expires and the value of the counter CFP6 (emergency private call cancel retransmission) is equal to the upper limit, the MCPTT client:

1) shall release the stored current call type;

2) shall release the stored Prose per-packet priority; and

3) shall enter "Q0: waiting for the call to be established".

11.2.3.4.6.5 Responding to emergency private call cancel

When in the "Q1: in-progress private call" state or "Q2: in-progress emergency private call" state, upon receiving a PRIVATE CALL EMERGENCY CANCEL message with the same "call identifier" IE, the MCPTT client:

1) shall generate a PRIVATE CALL EMERGENCY CANCEL ACK as specified in subclause 15.1.13:

   a) shall set the Call identifier IE to the stored call identifier;

   b) shall set the MCPTT user ID of the callee IE with own MCPTT user ID; and

   c) shall set the MCPTT user ID of the caller IE with MCPTT user ID of the caller IE in received message;

2) shall send PRIVATE CALL EMERGENCY CANCEL ACK message according to rules and procedures as specified in subclause 11.2.1.1.1;

3) shall stop TFP8 (implicit downgrade) timer;

4) shall establish a media session based on the SDP body of the stored answer SDP;

5) shall set the ProSe per-packet priority to the value corresponding to MCPTT off-network private call as described in 3GPP TS 24.483 [45]; and

6) shall enter the "Q1: in-progress private call" state and set the stored current call type to "PRIVATE CALL", if current state is the "Q2: in-progress emergency private call" state.

11.2.3.4.6A Implicit downgrade

When in the "Q2: in-progress emergency private call" state, upon expiry of TFP8 (implicit downgrade) timer, the MCPTT client:

1) shall establish a media session based on the SDP body of the stored answer SDP;

2) shall set the ProSe per-packet priority to the value corresponding to MCPTT off-network private call as described in 3GPP TS 24.483 [45];

3) shall set the stored current call type to "PRIVATE CALL"; and

4) shall enter the "Q1: in-progress private call" state.

11.2.3.4.7 Call Release

When in state "Q1: in-progress private call" or "Q2: in-progress emergency private call", upon receiving an indication from MCPTT user to release the call or upon receiving PRIVATE CALL RELEASE message, the MCPTT client:

1) shall release the stored current call type;

2) shall release the stored Prose per-packet priority; and

3) shall enter "Q0: waiting for the call to be established".

11.2.3.4.8 Error handling

11.2.3.4.8.1 Unexpected MONP message received

Upon receiving a MONP message in a state where there is no handling specified for the MONP message, the MCPTT client shall discard the MONP message.

11.2.3.4.8.2 Unexpected indication from MCPTT user

Upon receiving an indication from the MCPTT user in a state where there is no handling specified for the indication, the MCPTT client shall ignore the indication.

11.2.3.4.8.3 Unexpected expiration of a timer

Upon expiration of a timer in a state where there is no handling specified for expiration of the timer, the MCPTT client shall ignore the expiration of the timer.

12 Emergency alert

12.0 General

This subclause describes the emergency alert procedures for on-network and off-network.

For on-network emergency alert, the procedures for originating and terminating MCPTT clients, participating MCPTT functions and controlling MCPTT function are specified in subclause 12.1. MCPTT emergency call procedures that have emergency alerts as an optional capability shall be performed as defined in subclause 10.1 for on-network group call and defined in subclause 11.1 for on-network private call.

For off-network emergency alert, the procedures for each functional entity is specified in subclause 12.2.

12.1 On-network emergency alert

12.1.1 Client procedures

12.1.1.1 Emergency alert origination

Upon receiving a request from the MCPTT user to send an MCPTT emergency alert to the indicated MCPTT group and this is an authorised request for an MCPTT emergency alert as determined by subclause 6.2.8.1.6, the MCPTT client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] with the clarifications given below.

NOTE 1: this SIP MESSAGE request is assumed to be sent out-of-dialog.

The MCPTT client:

1) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP MESSAGE request;

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

3) may include a P-Preferred-Identity header field in the SIP MESSAGE request containing a public user identity as specified in 3GPP TS 24.229 [4];

4) shall include an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with:

   a) the <mcptt-request-uri> element set to the group identity;

   b) the <alert-ind> element set to a value of "true"; and

   c) the <mcptt-client-id> element set to the MCPTT client ID of the originating MCPTT client;

5) shall include in the SIP MESSAGE request the specific location information for MCPTT emergency alert as specified in subclause 6.2.9.1;

6) shall set the MCPTT emergency state if not already set;

7) shall set the MCPTT emergency alert state to "MEA 2: emergency-alert-confirm-pending";

8) shall set the Request-URI to the public service identity identifying the participating MCPTT function serving the group identity; and

9) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

On receiving a SIP 2xx response to the SIP MESSAGE request, the MCPTT client shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated".

On receiving a SIP 4xx response a SIP 5xx response or a SIP 6xx response to the SIP MESSAGE request, the MCPTT client shall set the MCPTT emergency alert state to "MEA 1: no-alert".

NOTE 2: the MCPTT emergency state is left set in this case as the MCPTT user presumably is in the best position to determine whether or not they are in a life-threatening condition. The assumption is that the MCPTT user can clear the MCPTT emergency state manually if need be.

12.1.1.2 Emergency alert cancellation

Upon receiving a request from the MCPTT user to send an MCPTT emergency alert cancellation to the indicated MCPTT group and this is an authorised request for an MCPTT emergency alert cancellation as determined by subclause 6.2.8.1.6, the MCPTT client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] with the clarifications given below.

NOTE 1: This SIP MESSAGE request is assumed to be sent out-of-dialog.

The MCPTT client:

1) 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-Preferred-Service header field according to IETF RFC 6050 [9] in the SIP MESSAGE request;

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

3) may include a P-Preferred-Identity header field in the SIP MESSAGE request containing the public user identity of the originator as specified in 3GPP TS 24.229 [4];

4) shall include an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with:

   a) the <mcptt-request-uri> element set to the MCPTT group identity;

   b) the <alert-ind> element set to a value of "false"; and

   c) if the MCPTT user is cancelling an MCPTT emergency alert originated by another MCPTT user, include the <originated-by> element set to the MCPTT ID of the MCPTT user who originated the MCPTT emergency alert;

5) if the MCPTT user has additionally requested the cancellation of the in-progress emergency state of the MCPTT group and this is an authorised request for an in-progress emergency group state cancellation as determined by

subclause 6.2.8.1.7, shall include an <emergency-ind> element set to a value of "false" in the <mcpttinfo> element containing the <mcptt-Params> element;

6) shall set the Request-URI to the public service identity identifying the participating MCPTT function serving the group identity;

7) if the generated SIP MESSAGE request does not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, shall set the MCPTT emergency alert state to "MEA 4: Emergency-alert-cancel-pending"; and

8) shall send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [4].

On receipt of a SIP MESSAGE request containing an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind-rcvd> element set to true and an <mcptt-client-id> matching the MCPTT client ID included in the sent SIP MESSAGE request:

1) if the <alert-ind> element is set to a value of "false" in the application/vnd.3gpp.mcptt-info+xml MIME body of the received SIP MESSAGE request and the sent SIP MESSAGE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, shall:

   a) set the MCPTT emergency alert state to "MEA 1: no-alert"; and

   b) clear the MCPTT emergency state if not already cleared;

2) if the <alert-ind> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the received SIP MESSAGE request is set to a value of "true" and if the MCPTT emergency alert state is set to "MEA 4: Emergency-alert-cancel-pending" and the sent SIP MESSAGE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated"; and

NOTE 2: It would appear to be an unusual situation for the initiator of an MCPTT emergency alert to not be able to clear their own alert. Nevertheless, an MCPTT user can be configured to be authorised to initiate MCPTT emergency alerts but not have the authority to clear them. Hence, the case is covered here.

3) if an <emergency-ind> element is present in the application/vnd.3gpp.mcptt-info+xml MIME body of received SIP MESSAGE request and is set to a value of "false":

   a) shall set the MCPTT emergency group call state of the group to "MEGC 1: emergency-gc-capable"; and

   b) shall set the MCPTT emergency group state of the group to "MEG 1: no-emergency".

NOTE 3: The case where an <emergency-ind> element is set to true is possible but not handled specifically above as it results in no state changes.

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the sent SIP MESSAGE request:

1) if the received SIP 4xx response, SIP 5xx response or SIP 6xx response contains an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <alert-ind> element set to a value of "true", the sent SIP MESSAGE request did not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body and the MCPTT emergency alert state is set to "MEA 4: Emergency-alert-cancel-pending", shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated"; and

NOTE 4: In this case, an <emergency-ind> element would either not be present or would be set to true. In either case, no change in state would result. Hence, this case is not specified above.

2) if the received SIP 4xx response, SIP 5xx response or a SIP 6xx response to the SIP MESSAGE request does not contain an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind> element, the sent SIP MESSAGE request does not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body and the MCPTT emergency alert state is set to "MEA 4: Emergency-alert-cancel-pending", shall set the MCPTT emergency alert state to "MEA 3: emergency-alert-initiated".

12.1.1.3 MCPTT client receives an MCPTT emergency alert or call notification

Upon receipt of a "SIP MESSAGE request for emergency notification", the MCPTT client:

1) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "true", should display to the MCPTT user an indication of the MCPTT emergency alert and associated information, including:

   a) the MCPTT group identity contained in <mcptt-calling-group-id> element application/vnd.3gpp.mcptt-info+xml MIME body;

   b) the originator of the MCPTT emergency alert contained in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

   c) the mission critical organization of the MCPTT emergency alert originator contained in the <mc-org> element of the application/vnd.3gpp.mcptt-info+xml MIME body;

NOTE 1: This is the case of the MCPTT client receiving the notification of another MCPTT user's emergency alert.

2) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "false":

   a) should display to the MCPTT user an indication of the MCPTT emergency alert cancellation and associated information, including:

      i) the MCPTT group identity contained in the <mcptt-calling-group-id> element application/vnd.3gpp.mcptt-info+xml MIME body;

      ii) the originator of the MCPTT emergency alert contained in:

         A) if present, the <originated-by> element of the application/vnd.3gpp.mcptt-info+xml MIME body; or

         B) the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

   b) if the MCPTT ID contained in the <originated-by> element is the MCPTT ID of the receiving MCPTT user, shall set the MCPTT emergency alert state to "MEA 1: no-alert"; and

   c) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <emergency-ind> element is set to a value of "false":

      i) shall set the MCPTT emergency group state to "MEG 1: no-emergency"; and

      ii) shall set the MCPTT emergency group call state to "MEGC 1: emergency-gc-capable";

NOTE 2: This is the case of the MCPTT client receiving the notification of the cancellation by a third party of an MCPTT emergency alert. This can be the MCPTT emergency alert of another MCPTT user or the MCPTT emergency alert of the recipient, as determined by the contents of the <originated-by> element. Optionally, notification of the cancellation of the in-progress emergency state of the MCPTT group can be included.

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

   a) should display to the MCPTT user an indication of the additional emergency MCPTT user participating in the MCPTT emergency group call including the following if not already displayed as part of step 1):

      i) the MCPTT group identity contained in the <mcptt-calling-group-id> element application/vnd.3gpp.mcptt-info+xml MIME body; and

      ii) the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body;

   b) shall set the MCPTT emergency group state to "MEG 2: in-progress" if not already set to that value;

NOTE 3: This is the case of the MCPTT client receiving notification of an additional MCPTT user in an MCPTT emergency state (i.e., not the MCPTT user that originally triggered the in-progress emergency state of the group) joining the in-progress emergency group call. An emergency alert indication, if included, is handled in step 1).

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

a) should display to the MCPTT user an indication of the cancellation of the in-progress emergency state of the MCPTT group call including the following if not already displayed as part of step 2):

i) the MCPTT group identity contained in the <mcptt-calling-group-id> element application/vnd.3gpp.mcptt-info+xml MIME body; and

ii) the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body;

b) shall set the MCPTT emergency group state to "MEG 1: no-emergency"; and

c) shall set the MCPTT emergency group call state to "MEGC 1: emergency-gc-capable";

NOTE 4: This is the case of the MCPTT client receiving the notification of the cancellation of the in-progress emergency state of the MCPTT group. In this case, the receiving MCPTT client is affiliated with the MCPTT group but not participating in the session. An emergency alert cancellation, if included, is handled in step 2).

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

a) should display to the MCPTT user an indication of the MCPTT user participating in the MCPTT imminent peril group call including the following if not already displayed as part of step 1):

i) the MCPTT group identity contained in the <mcptt-calling-group-id> element application/vnd.3gpp.mcptt-info+xml MIME body; and

ii) the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body; and

b) shall set the MCPTT imminent peril group state to "MIG 2: in-progress" if not already set to that value;

NOTE 5: This is the case of the MCPTT client receiving notification of an additional MCPTT user initiating an imminent peril group call when there is already an in-progress imminent peril state in effect on the group.

6) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <imminentperil-ind> element set to a value of "false":

a) should display to the MCPTT user an indication of the cancellation of the in-progress imminent peril state of the MCPTT group including the following if not already displayed as part of step 2):

i) the MCPTT group identity contained in the <mcptt-calling-group-id> element application/vnd.3gpp.mcptt-info+xml MIME body; and

ii) the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body;

b) shall set the MCPTT imminent peril group state to "MIG 1: no-imminent-peril"; and

c) shall set the MCPTT imminent peril group call state to "MIGC 1: imminent-peril-gc-capable";

NOTE 6: This is the case of the MCPTT client receiving notification of the cancellation of the in-progress imminent peril state of the group.

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

8) shall send the SIP 200 (OK) response towards the MCPTT server according to rules and procedures of 3GPP TS 24.229 [4].

12.1.2 Participating MCPTT function procedures

12.1.2.1 Receipt of a SIP MESSAGE request for emergency notification from the served MCPTT client

Upon receipt of a "SIP MESSAGE request for emergency notification for originating 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 MESSAGE 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 skip the rest of the steps;

NOTE 1: if the SIP MESSAGE request contains an emergency indication set to a value of "true" or an alert indication set to a value of "true", 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 the public user identity in the P-Asserted-Identity header field of the SIP MESSAGE 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 the MCPTT user is not affiliated with the MCPTT group as determined by subclause 9.2.2.2.11, shall perform the actions specified in subclause 9.2.2.2.12 for implicit affiliation;

4) if the actions for implicit affiliation specified in step 3) 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 MESSAGE request for emergency notification 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 3: N2 is the total number of MCPTT groups that an MCPTT user can be affiliated to simultaneously as specified in 3GPP TS 23.379 [3].

NOTE 4: As this is a request for MCPTT emergency services, the participating MCPTT function can choose to accept the request.

5) shall determine the public service identity of the controlling MCPTT function associated with the group identity in the received SIP MESSAGE request;

6) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

7) shall set the Request-URI of the outgoing SIP MESSAGE request to the public service identity of the controlling MCPTT function associated with the group identified by the <mcptt-request-uri> element contained in the <mcpttinfo> element containing the <mcptt-Params> element of the application/vnd.3gpp.mcptt-info+xml MIME body in the incoming SIP MESSAGE request;

8) shall copy the contents of the application/vnd.3gpp. mcptt-info+xml MIME body in the received SIP MESSAGE request into an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 included in the outgoing SIP MESSAGE request;

9) shall set the <mcptt-calling-user-id> element of the <mcpttinfo> element containing the <mcptt-Params> element to the MCPTT ID determined in step 2) above;

10) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in clause F.3 shall copy the contents of the application/vnd.3gpp.mcptt-location-info+xml MIME body in the received SIP MESSAGE request into an application/vnd.3gpp.mcptt-location-info+xml MIME body included in the outgoing SIP MESSAGE request;

11) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public user identity in the P-Asserted-Identity header field contained in the received SIP MESSAGE request; and

12) shall send the SIP MESSAGE request as specified to 3GPP TS 24.229 [4].

Upon receipt of a SIP 2xx response in response to the SIP MESSAGE request sent in step 10):

1) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.229 [4] with the follow clarifications:

   a) shall include the public user 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;

2) 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; and

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

Upon receipt of a SIP 4xx, 5xx or 6xx response to the sent SIP MESSAGE request and if the implicit affiliation procedures of subclause 9.2.2.2.12 were invoked in the present subclause, the participating MCPTT function shall perform the procedures of subclause 9.2.2.2.14.

12.1.2.2 Receipt of a SIP MESSAGE request for emergency notification for terminating MCPTT client

In the procedures in this subclause:

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

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

Upon receipt of a "SIP MESSAGE requests for emergency notification 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 MESSAGE 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 skip the rest of the steps;

NOTE 1: if the SIP MESSAGE request contains an emergency indication set to a value of "true" or an alert indication set to a value of "true", the participating MCPTT function can by means beyond the scope of this specification choose to accept the request.

2) 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 MESSAGE request to retrieve the binding between the MCPTT ID and public user identity;

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

4) shall generate an outgoing SIP MESSAGE request as specified in subclause 6.3.2.2.11; and

5) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the participating MCPTT function shall follow the procedures specified in 3GPP TS 24.229 [4].

12.1.2.3 Receipt of a SIP MESSAGE request indicating successful delivery of emergency notification

Upon receipt of a SIP MESSAGE request routed to the terminating participating MCPTT function as a result of initial filter criteria with the Request-URI set to the public service identity of the terminating participating MCPTT function and the SIP MESSAGE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with an <alert-ind-rcvd> element present, 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 MESSAGE 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 skip the rest of the steps;

2) 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 MESSAGE request to retrieve the binding between the MCPTT ID and public user identity;

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

4) shall generate an outgoing SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33] and:

   a) shall include in the SIP MESSAGE 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] that were received (if any) in the incoming SIP MESSAGE request;

   b) shall set the Request-URI of the outgoing SIP MESSAGE request to the public user identity associated to the MCPTT ID of the MCPTT user that was in the Request-URI of the incoming SIP MESSAGE request;

   c) shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body received in the incoming SIP MESSAGE request into an application/vnd.3gpp.mcptt-info+xml MIME body included in the outgoing SIP MESSAGE request; and

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

5) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the participating MCPTT function shall follow the procedures specified in 3GPP TS 24.229 [4].

12.1.3 Controlling MCPTT function procedures

12.1.3.1 Handling of a SIP MESSAGE request for emergency notification

Upon receipt of a "SIP MESSAGE request for emergency notification for controlling MCPTT function", the controlling 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 MESSAGE request with a SIP 500 (Server Internal Error) response. The controlling 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: If the SIP MESSAGE request contains an alert indication set to a value of "true", the controlling MCPTT function can, according to local policy, choose to accept the request.

2) shall reject the SIP request with a SIP 403 (Forbidden) response and not process the remaining steps if an Accept-Contact header field does not include the g.3gpp.icsi-ref media feature tag containing the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt";

3) if the received SIP MESSAGE request contains an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "false", shall perform the procedures specified in subclause 12.1.3.2 and skip the rest of the steps;

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

   a) if the received SIP MESSAGE request is an unauthorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1 shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request as specified in 3GPP TS 24.229 [4] with the following clarifications:

      i) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <alert-ind> element set to a value of "false"; and

      ii) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4] and skip the rest of the steps; and

   b) if the received SIP MESSAGE request is an authorised request for an MCPTT emergency alert as specified in subclause 6.3.3.1.13.1:

i) if the sending MCPTT user identified by the <mcptt-calling-user-id> element included in the application/vnd.3gpp.mcptt-info+xml MIME body is not affiliated with the MCPTT group identified by the <mcptt-request-uri> element of the MIME body as determined by the procedures of subclause 6.3.6:

I) shall check if the MCPTT user is eligible to be implicitly affiliated with the MCPTT group as determined by subclause 9.2.2.3.6;

II) if the MCPTT user is determined not to be eligible to be implicitly affiliated to the MCPTT group shall reject the SIP MESSAGE request with 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; or

III) if the procedures of subclause 9.2.2.3.6 determined the MCPTT user to be eligible to be implicitly affiliated to the MCPTT group shall, perform the implicit affiliation as specified in subclause 9.2.2.3.7;

ii) for each of the other affiliated members of the group:

A) generate an outgoing SIP MESSAGE request notification of the MCPTT user's emergency alert indication as specified in subclause 6.3.3.1.11 with the clarifications of subclause 6.3.3.1.12;

B) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <mcptt-calling-user-id> element set to the value of the <mcptt-calling-user-id> element in the received SIP MESSAGE request; and

C) send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [4];

iii) shall generate a SIP 200 (OK) response to the received SIP MESSAGE request as specified in 3GPP TS 24.229 [4] with the following clarifications:

A) shall cache the information that the MCPTT user has initiated an MCPTT emergency alert;

iv) shall send the SIP 200 (OK) response to the received SIP MESSAGE according to rules and procedures of 3GPP TS 24.229 [4].

v) shall generate a SIP MESSAGE request as described in subclause 6.3.3.1.20 to indicate successful receipt of an emergency alert, and shall include in the application/vnd.3gpp.mcptt-info+xml MIME body:

A) the <alert-ind> element set to a value of "true";

B) the <alert-ind-rcvd> element set to a value of true; and

C) the <mcptt-client-id> element with the MCPTT client ID that was included in the incoming SIP MESSAGE request; and

vi) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [4].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the controlling MCPTT function shall follow the procedures specified in 3GPP TS 24.229 [4].

12.1.3.2 Handling of a SIP MESSAGE request for emergency alert cancellation

Upon receipt of a "SIP MESSAGE request for emergency notification for controlling MCPTT function" containing an application/vnd.3gpp.mcptt-info+xml MIME body with the <alert-ind> element set to a value of "false", the controlling MCPTT function:

1) if the received SIP MESSAGE request is an unauthorised request for an MCPTT emergency alert cancellation as specified in subclause 6.3.3.1.13.1:

a) and if the received SIP MESSAGE request does not contain an <emergency-ind> element or is an unauthorised request for an MCPTT emergency call cancellation as specified in subclause 6.3.3.1.13.4, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request as specified in 3GPP TS 24.229 [4] with the following clarifications:

i) shall include in the SIP 403 (Forbidden) response an application/vnd.3gpp.mcptt-info+xml MIME body as specified in clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <alert-ind> element set to a value of "true";

ii) if the received SIP MESSAGE request contains an <emergency-ind> element of the <mcpttinfo> element set to a value of "false" and if the in-progress emergency state of the group is set to a value of "true" and this is an unauthorised request for an MCPTT emergency call cancellation as determined in step i) above, shall include an <emergency-ind> element set to a value of "true" in the application/vnd.3gpp.mcptt-info+xml MIME body in the SIP 403 (Forbidden) response; and

iii) shall send the SIP 403 (Forbidden) response according to rules and procedures of 3GPP TS 24.229 [4] and skip the rest of the steps; and

b) and if the received SIP MESSAGE request contains an <emergency-ind> element and is an authorised request for an MCPTT emergency call cancellation as specified in subclause 6.3.3.1.13.4 and the in-progress emergency state of the MCPTT group is set to a value of "true":

i) shall set the in-progress emergency state of the group to a value of "false";

ii) shall clear the cache of the MCPTT ID of the MCPTT user that triggered the setting of the in-progress emergency state of the MCPTT group to "true";

iii) shall generate SIP re-INVITE requests to the other affiliated and joined members of the MCPTT group as specified in subclause 6.3.3.1.6. The MCPTT controlling function:

A) for each affiliated and joined member shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

B) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5];

iv) for each of the affiliated but not joined members of the group shall:

A) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's emergency call as specified in subclause 6.3.3.1.11;

B) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <mcptt-calling-user-id> element set to the value of the <mcptt-calling-user-id> element in the received SIP MESSAGE request; and

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

v) shall generate a SIP 200 (OK) response to the received SIP MESSAGE request as specified in 3GPP TS 24.229 [4];

vi) shall send the SIP 200 (OK) response to the received SIP MESSAGE as specified in 3GPP TS 24.229 [4] and skip the rest of the steps;

vii) shall generate a SIP MESSAGE request as described in subclause 6.3.3.1.20 to indicate successful receipt of the request for emergency alert cancellation

viii) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP MESSAGE request:

A) the <alert-ind> element set to a value of "true";

B) the <alert-ind-rcvd> element set to a value of true;

C) the <emergency-ind> element set to a value of "false"; and

D) the <mcptt-client-id> element with the MCPTT client ID that was included in the incoming SIP MESSAGE request; and

ix) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [4]; and

2) if the received SIP MESSAGE request is an authorised request for an MCPTT emergency alert cancellation as specified in subclause 6.3.3.1.13.1:

   a) if the received SIP MESSAGE request contains an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, shall clear the cache of the MCPTT ID of the MCPTT user identified by the <originated-by> element as having an outstanding MCPTT emergency alert;

   b) if the received SIP MESSAGE request does not contain an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, clear the cache of the MCPTT ID of the sender of the SIP MESSAGE request as having an outstanding MCPTT emergency alert;

   c) if the received SIP MESSAGE request does not contain an <emergency-ind> element or is an unauthorised request for an MCPTT emergency call cancellation as specified in subclause 6.3.3.1.13.4, for each of the affiliated but not joined members of the group shall:

      i) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's emergency alert as specified in subclause 6.3.3.1.11;

      ii) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <mcptt-calling-user-id> element set to the value of the <mcptt-calling-user-id> element in the received SIP MESSAGE request;

      iii) if the received SIP MESSAGE request contains an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, copy the contents of the received <originated-by> element to an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP MESSAGE request;

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

      v) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4];

   d) if the received SIP MESSAGE request contains an <emergency-ind> element and is an authorised request for an MCPTT emergency call cancellation as specified in subclause 6.3.3.1.13.4 and the in-progress emergency state of the MCPTT group is set to a value of "true":

      i) shall set the in-progress emergency state of the group to a value of "false";

      ii) cache the information that the MCPTT user has cancelled the outstanding in-progress emergency state of the group;

      iii) shall generate SIP re-INVITES requests to the other affiliated and joined members of the MCPTT group as specified in subclause 6.3.3.1.6. The MCPTT controlling function:

         A) for each affiliated and joined member shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [4]; and

         B) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the controlling MCPTT function shall interact with the media plane as specified in 3GPP TS 24.380 [5]; and

      iv) for each of the affiliated but not joined members of the group shall:

         A) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's emergency call as specified in subclause 6.3.3.1.11;

         B) include in the application/vnd.3gpp.mcptt-info+xml MIME body with the <mcpttinfo> element containing the <mcptt-Params> element with the <mcptt-calling-user-id> element set to the value of the <mcptt-calling-user-id> element in the received SIP MESSAGE request;

         C) if the received SIP MESSAGE request contains an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body, copy the contents of the received <originated-by> element to an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP MESSAGE request;

         D) include in the application/vnd.3gpp.mcptt-info+xml MIME body an <alert-ind> element set to a value of "false"; and

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

e) shall generate a SIP 200 (OK) response to the received SIP MESSAGE request as specified in 3GPP TS 24.229 [4];

f) shall send the SIP 200 (OK) response to the received SIP MESSAGE as specified in 3GPP TS 24.229 [4].

g) shall generate a SIP MESSAGE request as described in subclause 6.3.3.1.20 to indicate successful receipt of the request for emergency alert cancellation;

h) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body, the <alert-ind> element set to a value of "false" and the <alert-ind-rcvd> set to "true";

i) shall populate the <mcptt-client-id> element with the MCPTT client ID that was included in the incoming SIP MESSAGE request;

j) if the received SIP MESSAGE request contains an <emergency-ind> element of the <mcpttinfo> element set to a value of "false":

i) if this is an authorised request for an MCPTT emergency call cancellation as specified in subclause 6.3.3.1.13.4, shall include an <emergency-ind> element set to a value of "false" in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP MESSAGE request; and

B) otherwise, if this is an unauthorised request for an MCPTT emergency call cancellation as specified in subclause 6.3.3.1.13.4, and the in-progress emergency state of the group is set to a value of "true", shall include an <emergency-ind> element set to a value of "true" in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP MESSAGE request; and

k) shall send the SIP MESSAGE request according to according to the rules and procedures of 3GPP TS 24.229 [4].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the controlling MCPTT function shall follow the procedures specified in 3GPP TS 24.229 [4].

12.2 Off-network emergency alert

12.2.1 General

12.2.2 Basic state machine

12.2.2.1 General

12.2.2.2 Emergency alert state machine

The figure 12.2.2.2-1 gives an overview of the main states and transitions on the UE for emergency alert.

Each emergency alert state machine is per MCPTT group.

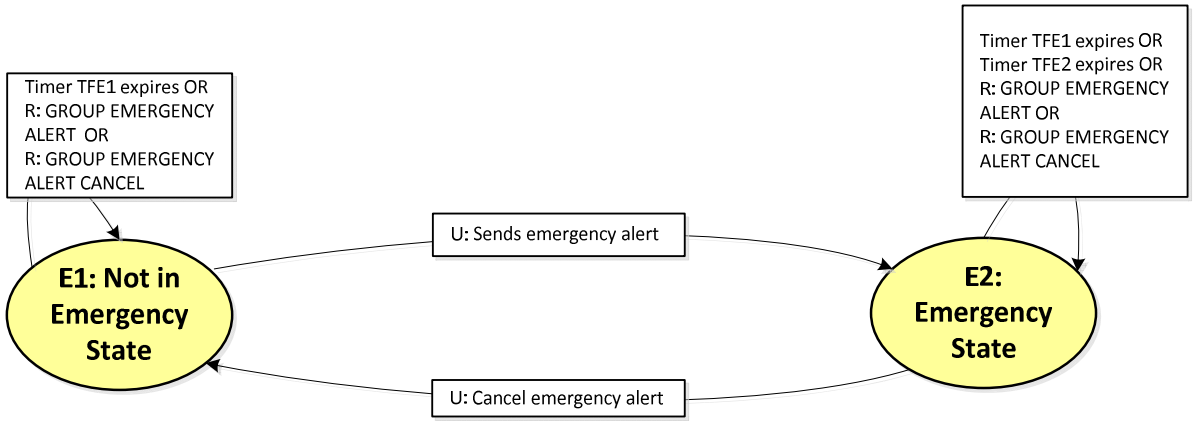

Figure 12.2.2.2-1: Emergency alert state machine

The following pieces of information are associated with the emergency alert state machine:

a) the stored emergency state of the MCPTT group; and

b) the stored organization name of the MCPPT client.

NOTE: The emergency alert state machine is referred by the MCPTT off-network group call and MCPTT off-network private call procedures.

12.2.2.3 Emergency alert states

12.2.2.3.1 E1: Not in emergency state

This state is the start state of this state machine.

The UE stays in this state while not in emergency state.

12.2.2.3.2 E2: Emergency state

This state exists for UE, when the UE has sent a GROUP EMERGENCY ALERT message.

12.2.3 Procedures

12.2.3.1 Originating user sending emergency alert

When in state "E1: Not in emergency state", upon receiving an indication from the MCPTT user to transmit an emergency alert for an MCPTT group ID, and the values of "/<*x*>/<*x*>/Common/MCPTTGroupCall/EmergencyAlert/Authorised" leaf node present in the user profile and "/<*x*>/<x>/Common/AllowedEmergencyAlert" present in group configuration as specified in 3GPP TS 24.483 [45] are set to "true", the MCPTT client:

1) shall set the stored emergency state as "true";

2) shall set the stored MCPTT group ID to the indicated MCPTT group ID;

3) shall generate a GROUP EMERGENCY ALERT message as specified in subclause 15.1.16. In the GROUP EMERGENCY ALERT message, the MCPTT client:

   a) shall set the MCPTT group ID IE to the stored MCPTT group ID;

   b) shall set the Originating MCPTT user ID IE to own MCPTT user ID;

   c) shall set the Organization name IE to own organization name; and

d) may set the User location IE with client's current location, if requested;

4) shall send the GROUP EMERGENCY ALERT message as specified in subclause 10.2.1.1.1;

5) shall start timer TFE2 (emergency alert retransmission); and

6) shall enter "E2: Emergency state" state.

12.2.3.2 Emergency alert retransmission

When in state "E2: Emergency state", upon expiry of timer TFE2 (emergency alert retransmission), the MCPTT client:

1) shall generate a GROUP EMERGENCY ALERT message as specified in subclause 15.1.16. In the GROUP EMERGENCY ALERT message, the MCPTT client:

   a) shall set the MCPTT group ID IE to the stored MCPTT group ID;

   b) shall set the originating MCPTT user ID IE to own MCPTT user ID;

   c) shall set the Organization name IE to own organization name; and

   d) may set the Location IE with client's current location, if requested; and

2) shall send the GROUP EMERGENCY ALERT message as specified in subclause 10.2.1.1.1;

3) shall start the timer TFE2 (emergency alert retransmission); and

4) shall remain in the current state.

12.2.3.3 Terminating user receiving emergency alert

When in state "E1: Not in emergency state" or in "E2: Emergency state", upon receiving a GROUP EMERGENCY ALERT message with the Originating MCPTT user ID IE not stored in the list of users in emergency, the MCPTT client:

1) shall store the Originating MCPTT user ID IE and location IE in the list of users in emergency;

2) shall generate a GROUP EMERGENCY ALERT ACK message as specified in subclause 15.1.17. In the GROUP EMERGENCY ALERT ACK message, the MCPTT client:

   a) shall set the MCPTT group ID IE to the MCPTT group ID IE of the received GROUP EMERGENCY ALERT message;

   b) shall set the Sending MCPTT user ID IE to own MCPTT user ID; and

   c) shall set the Originating MCPTT user ID IE to the Originating MCPTT user ID IE of the received GROUP EMERGENCY ALERT message; and

3) shall send the GROUP EMERGENCY ALERT ACK message as specified in subclause 10.2.1.1.1;

4) shall start timer TFE1 (emergency alert); and

5) shall remain in the current state.

NOTE: Each instance of timer TFE1 is per MCPTT user ID.

12.2.3.4 Terminating user receiving retransmitted emergency alert

When in state "E1: Not in emergency state" or in "E2: Emergency state", upon receiving a GROUP EMERGENCY ALERT message with the Originating MCPTT user ID IE stored in the list of users in emergency, the MCPTT client:

1) may update the stored location of the user with the received Location IE;

2) shall restart the associated timer TFE1 (emergency alert); and

3) shall remain in the current state.

12.2.3.5 Originating user cancels emergency alert

When in "E2: Emergency state", upon receiving an indication from the MCPTT user to cancel an emergency alert and the value of "/<*x*>/<*x*>/Common/MCPTTGroupCall/EmergencyAlert/Cancel" leaf node present in the user profile as specified in 3GPP TS 24.483 [45] set to "true", the MCPTT client:

1) shall set the stored emergency state as "false";

2) shall generate a GROUP EMERGENCY ALERT CANCEL message as specified in subclause 15.1.18. In the GROUP EMERGENCY ALERT CANCEL message, the MCPTT client:

   a) shall set the MCPTT group ID IE to the stored MCPTT group ID;

   b) shall set the Originating MCPTT user ID IE to own MCPTT user ID; and

   c) shall set the Sending MCPTT user ID IE to own MCPTT user ID;

3) shall send the GROUP EMERGENCY ALERT CANCEL message as specified in subclause 10.2.1.1.1;

4) shall stop timer TFE2 (emergency alert retransmission); and

5) shall enter "E1: Not in emergency state" state.

12.2.3.6 Terminating user receives GROUP EMERGENCY ALERT CANCEL message

When in state "E1: Not in emergency state" or in "E2: Emergency state", upon receiving a GROUP EMERGENCY ALERT CANCEL message with the Originating MCPTT user ID IE stored in the list of users in emergency, the MCPTT client:

1) shall remove the MCPTT user ID and associated location information from the stored list of users in emergency;

2) shall generate a GROUP EMERGENCY ALERT CANCEL ACK message as specified in subclause 15.1.19. In the GROUP EMERGENCY ALERT CANCEL ACK message, the MCPTT client:

   a) shall set the MCPTT group ID IE to the MCPTT group ID IE of the received GROUP EMERGENCY ALERT CANCEL message; and

   b) shall set the Sending MCPTT user ID IE to own MCPTT user ID; and

   c) shall set the Originating MCPTT user ID IE to the Originating MCPTT user ID IE of the received GROUP EMERGENCY ALERT message;

3) shall send the GROUP EMERGENCY ALERT CANCEL ACK message as specified in subclause 10.2.1.1.1;

4) shall stop the associated timer TFE1 (emergency alert); and5) shall remain in the current state.

12.2.3.7 Implicit emergency alert cancel

When in state "E1: Not in emergency state" or in "E2: Emergency state", upon expiry of timer TFE1 (emergency alert) associated with a stored MCPTT user ID, the MCPTT client:

1) shall remove the MCPTT user ID and associated location information from the stored list of users in emergency; and

2) shall remain in the current state.

13 Location procedures

13.1 General

If the participating MCPTT function needs to obtain location information, the participating MCPTT function configures the MCPTT client when the participating MCPTT function receives a third-party REGISTER request where the MCPTT client SIP URI is in the To header field. The configuration contains information the MCPTT client uses to set up filter criteria for when the MCPTT client shall send location reports to the participating MCPTT function.

The participating MCPTT function can also explicitly request the MCPTT client to send a location report.

The MCPTT client will, based on the received configuration or when explicitly requested, send location reports.

The location information is used by the participating MCPTT function to determine whether to use MBMS bearers or not as described in clause 14.

13.2 Participating MCPTT function location procedures

13.2.1 General

The participating MCPTT function has procedures to:

- configure the location reporting at the UE;
- request the UE to report the location of the UE; and
- receive a location information report from the UE.

13.2.2 Location reporting configuration

Upon receipt of a third-party SIP REGISTER request for an MCPTT client, the participating MCPTT function may configure the location reporting in the MCPTT client by generating a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33]. The participating MCPTT function:

1) shall include a Request-URI set to the URI received in the To header field in the third-party SIP REGISTER request;
2) shall include an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref set to the value "urn:urn-7:3gpp-service.ims.icsi.mcptt" along with parameters "require" and "explicit" in accordance with IETF RFC 3841 [6];
3) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with an <mcptt-request-uri> element containing the MCPTT ID of the MCPTT user to receive the configuration;
4) shall include an application/vnd.3gpp.mcptt-location-info+xml MIME body with the <Configuration> element contained in the <location-info> root element set to the desired configuration;
5) shall include the TriggerId attribute where defined for the sub-elements defining the trigger criterion ;
6) shall include the public service identity of the participating MCPTT function in the P-Asserted-Identity header field;
7) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and
8) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4].

13.2.3 Location information request

If the participating MCPTT function needs to request the MCPTT client to report its location, the participating MCPTT functions shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33]. The participating MCPTT function:

1) shall include a Request-URI set to the URI received in the To header field in the third-party SIP REGISTER request;

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

3) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with an <mcptt-request-uri> element containing the MCPTT ID of the MCPTT user;

4) shall include an application/vnd.3gpp.mcptt-location-info+xml MIME body with a <Request> element contained in the <location-info> root element;

5) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

6) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4].

13.2.4 Location information report

If the participating MCPTT function receives a SIP request containing:

1) a Content-Type header field set to "application/vnd.3gpp.mcptt-location-info+xml"; and

2) an application/vnd.3gpp.mcptt-location-info+xml MIME body with a <Report> element included in the <location-info> root element;

then the participating MCPTT function shall authorise the location report based on the MCPTT ID received. If the MCPTT user is authorised to send a location report the participating MCPTT function:

1) shall use the location information as needed.

NOTE: The <Report> element contains the event triggering identity in the location information report from the UE, and can contain location information.

13.2.5 Abnormal cases

Upon receipt of a SIP request:

1) where the P-Asserted-Identity identifies a public user identity not associated with an MCPTT user served by the participating MCPTT function; or

2) with a MIME body with Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml" and with a <mcptt-request-URI> element containing an MCPTT ID that identifies an MCPTT user served by the participating MCPTT function;

then, when the SIP request contains:

1) an Accept-Contact header field with the g.3gpp.mcptt media feature tag;

2) an Accept-Contact header field with the g.3gpp.icsi-ref media-feature tag with the value of "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

3) an application/vnd.3gpp.mcptt-location-info+xml MIME body containing a <Request> element or a <Configuration> element;

the participating MCPTT function shall remove the application/vnd.3gpp.mcptt-location-info+xml MIME body from the outgoing SIP request.

13.3 MCPTT client location procedures

13.3.1 General

The MCPTT client sends a location report when one of the trigger criteria is fulfilled or when it receives a request from the participating MCPTT function to send a location report. To send the location report the MCPTT client can use an appropriate SIP message that it needs to send for other reasons, or it can include the location report in a SIP MESSAGE request.

To send a location report, the MCPTT client includes in the SIP MESSAGE request an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in clause F.3. The MCPTT client populates the elements in accordance with its reporting configuration. Further location information may also be included in the P-Access-Network-Info header field.

13.3.2 Location reporting configuration

Upon receiving a SIP MESSAGE request containing:

1) an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref set to the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

2) a Content-Type header field set to "application/vnd.3gpp.mcptt-location-info+xml"; and

3) an application/vnd.3gpp.mcptt-location-info+xml MIME body with a <Configuration> root element included in the <location-info> root element;

then the MCPTT client:

1) shall store the contents of the <Configuration> elements;

2) shall set the location reporting triggers accordingly; and

3) shall start the minimumReportInterval timer.

13.3.3 Location information request

Upon receiving a SIP MESSAGE request containing

1) an Accept-Contact header field with the media feature tag g.3gpp.icsi-ref set to the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

2) a Content-Type header field set to "application/vnd.3gpp.mcptt-location-info+xml"; and

3) an application/vnd.3gpp.mcptt-location-info+xml MIME body with a <Request> element included in the <location-info> root element;

then the MCPTT client:

1) shall send a location report as specified in subclause 13.3.4; and

2) shall reset the minimumReportInterval timer.

13.3.4 Location information report

13.3.4.1 Report triggering

If a location reporting trigger fires the MCPTT client checks if the minimumReportInterval timer is running. If the timer is running the MCPTT client waits until the timer expires. When the minimumReportInterval timer fires, the MCPTT client:

1) shall, if any of the reporting triggers are still true, send a location information report as specified in subclause 13.3.4.2.

If the MCPTT client receives a location information request as specified in subclause 13.3.3, the MCPTT client shall send a location report as specified in subclause 13.3.4.2.

13.3.4.2 Sending location information report

If the MCPTT client needs to send a SIP request for other reasons (e.g. a SIP MESSAGE request containing an MBMS listening report as described in clause 14), the MCPTT client:

1) shall include an application/vnd.3gpp.mcptt-location-info+xml MIME body and in the <location-info> root element the MCPTT client shall include:

   a) a <Report> element and if the Report was triggered by a location request include the <ReportID> attribute set to the value of the <RequestID> attribute in the received Request;

   b) <TriggerId> child elements, where each element is set to the value of the <Trigger-Id> attribute associated with the trigger that have fired; and

   c) the location reporting elements corresponding to the triggers that have fired;

2) shall set the minimumReportInterval timer to the minimumReportInterval time and start the timer; and

3) shall reset all triggers.

If the MCPTT client does not need to send a SIP request for other reasons, the MCPTT client shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33]. The MCPTT client;

1) shall include in the Request-URI, the SIP URI received in the P-Asserted-Identity header field in the received SIP MESSAGE request for location report configuration;

2) shall include a Content-Type header field set to "application/vnd.3gpp.mcptt-location-info+xml";

3) shall include an application/vnd.3gpp.mcptt-location-info+xml MIME body and in the <location-info> root element include:

   a) a <Report> element and if the Report was triggered by a location request include the <ReportID> attribute set to the value of the <RequestID> attribute in the received Request;

   b) a <TriggerId> child element set to the value of each <Trigger-Id> value of the triggers that have fired; and

   c) the location reporting elements corresponding to the triggers that have fired;

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

5) shall set the minimumReportInterval timer to the minimumReportInterval time and start the timer;

6) shall reset all triggers; and

7) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [4].

14 MBMS transmission usage procedure

14.1 General

This clause describes the participating MCPTT function and the MCPTT client procedure for:

1) MBMS bearer announcements;

2) MBMS bearer listening status; and

3) MBMS bearer suspension status.

14.2 Participating MCPTT function MBMS usage procedures

14.2.1 General

This subclause describes the procedures in the participating MCPTT function for:

1) sending an MBMS bearer announcements to the MCPTT client;

2) receiving an MBMS bearer listening status from the MCPTT client; and

3) receiving an MBMS bearer suspension status from the MCPTT client.

14.2.2 Sending MBMS bearer announcement procedures

14.2.2.1 General

The availability of a MBMS bearer is announced to MCPTT clients by means of an MBMS bearer announcement message. One or more MBMS bearer announcement elements are included in an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body.

An MBMS bearer announcement message can contain new MBMS bearer announcements, updated MBMS bearer announcements or cancelled MBMS bearer announcements or a mix of all of them at the same time in an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body. Each initial MBMS bearer announcement message announces one MBMS bearer intended to carry a general purpose MBMS subchannel used for application level multicast signalling in a specified MBMS service area and additionally, the message could also announce zero or more extra MBMS bearers intended to carry media and media control.

NOTE: A new MBMS bearer announcement does not implicitly remove previously sent MBMS bearer announcements if the previously sent MBMS bearer announcement is not included in an MBMS bearer announcement message. However, the application/sdp MIME body, if included in the new MBMS bearer announcement message, fully replaces the existing application/sdp MIME body (which includes the MSCCK security key used to protect the general purpose MBMS subchannel).

When and to whom the participating MCPTT function sends the MBMS bearer announcement is based on local policy in the participating MCPTT function.

The following subclauses describe how the participating MCPTT function:

1. sends an initial MBMS bearer announcement message;

2. updates a previously sent announcement of MBMS bearer(s);

3. cancels a previously sent announcement of MBMS bearer(s); and

4. keys, re-keys or un-keys MCPTT groups using Multicast Signalling Key (MuSiK) via a key download procedure.

Prior to the participating MCPTT function transmitting on an MBMS bearer, the participating MCPTT function:

1. if necessary, shall instruct the local key management client to request keying material from the key management server as described in 3GPP TS 33.180 [78];

2. shall generate MSCCK(s) with the corresponding MSCCK-ID(s) and MuSiK(s) with the corresponding MuSiK-ID(s) as necessary; and

3. shall distribute MSCCKs, MSCCK-IDs, MuSiKs and MuSiK-IDs to the MCPTT clients, as needed, using the keying material received from the key management server for security protection, as described in 3GPP TS 33.180 [78].

14.2.2.2 Sending an initial MBMS bearer announcement procedure

For each MCPTT client that the participating MCPTT function is sending an MBMS bearer announcement to, the participating MCPTT function:

1) shall generate an SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

2) shall set the Request-URI to the URI received in the To header field in a third-party SIP REGISTER request;

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

4) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

5) shall include one application/sdp MIME body conforming to 3GPP TS 24.229 [4] where the application/sdp MIME body and:

   a) shall include the Content-Disposition header field with the value "render"; and

   b) should include one or more" m=audio" media lines and media line attributes as defined in 3GPP TS 24.380 [5] to be used as the MBMS subchannel for audio and media control. Additional the participating MCPTT function:

      i) shall set c-line to the unspecified address (0.0.0.0), if IPv4, or to a domain name within the ".invalid" DNS top-level domain, if IPv6;

      ii) shall set port number of the media line to 9;

      ii) shall include the "a=rtp-mux" attribute as specified in IETF RFC 5761 [39]; and

      iii) shall include the "a=rtcp:9" as specified in IETF RFC 5761 [39].

   c) should include one or more" m=audio" media lines and media line attributes as defined in 3GPP TS 24.380 [5] to be used as the MBMS subchannel for audio only. Additional the participating MCPTT function:

      i) shall set the c-line to the unspecified address (0.0.0.0), if IPv4, or to a domain name within the ".invalid" DNS top-level domain, if IPv6; and

      ii) shall set the port number of the media line to 9;

NOTE 1: If an MBMS subchannel for audio only is included, the "a=rtp-mux" and "a=rtcp:" attributes are not included in the media line.

   d) shall include one "m=application" media line as defined in 3GPP TS 24.380 [5] to be used as the general purpose MBMS subchannel. The media line shall include a valid multicast IP address and a valid port number. If the protection of MBMS subchannel control messages sent over the general purpose MBMS subchannel of the MBMS bearer is required, the participating MCPTT function also includes an "a=key-mgmt" media-level attribute. The participating MCPTT function:

      i) shall encrypt the MSCCK to a UID associated to the targeted MCPTT ID and a time related parameter as described in 3GPP TS 33.179 [46];

      ii) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated MSCCK and MSCCK-ID as specified in 3GPP TS 33.179 [46];

      iii) shall add the public service identity of the participating MCPTT function to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.179 [46];

      iv) shall sign the MIKEY-SAKKE I_MESSAGE using the public service identity of the participating MCPTT function signing key provided in the keying material together with a time related parameter, and add this to the MIKEY-SAKKE payload, as described in 3GPP TS 33.179 [46]; and

      v) shall include the "mikey" key management and protocol identifier and the signed MIKEY-SAKKE I_MESSAGE in the value of the a=key-mgmt" media-level attribute according to IETF RFC 4567 [47]; and

NOTE 2: The media parameters to be used by the MBMS subchannel for media is included in the Map Group To Bearer message defined in 3GPP TS 24.380 [5] and not included in this application/sdp MIME body.

e) if "m=audio" media lines to be used in an MBMS subchannel for audio only are included above, shall include one or more "m=application" media line as defined in 3GPP TS 24.380 [5] to be used as the MBMS subchannel for floor control messages. The media line:

i) shall set c-line to the unspecified address (0.0.0.0), if IPv4, or to a domain name within the ".invalid" DNS top-level domain, if IPv6; and

ii) shall set the port number of the media line to 9;

NOTE 3: The use of a separate MBMS subchannel for floor control is optional. When a separate MBMS subchannel for floor control is not used, floor control messages are sent in the MBMS subchannel for media.

6) shall include an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body defined in clause F.2 with the <version> element set to "1" and one or more <announcement> elements associated with the pre-activated MBMS bearers. Each set of an <announcement> element:

a) shall include a TMGI value in the <TMGI> element;

NOTE 4: The same TMGI value can only appear in one <announcement> element. The TMGI value is also used to identify the <announcement> when updating or cancelling the <announcement> element.

NOTE 5: The security key active for the general purpose MBMS subchannel on which the mapping (i.e. the MapGroupToBearer message) of media or media control to this MBMS bearer was indicated, is used for MBMS subchannels on this MBMS bearer, unless a different key or an indication of not using encryption is in place.

b) shall include the QCI value in the <QCI> element;

c) if multiple carriers are supported, shall include the frequency to be used in the <frequency> element;

NOTE 6: In the current release if the <frequency> element is included, the frequency in the <frequency> element is the same as the frequency used for unicast.

d) shall include one or more MBMS service area IDs in the <mbms-service-areas> element;

NOTE 7: Initial mappings of groups to MBMS subchannels on an MBMS bearer for the purpose of carrying media or media control can occur only where the MBMS service area for this bearer and the MBMS service area for the bearer carrying the general purpose MBMS subchannel on which the MapGroupToBearer message is sent intersect. However, once media or media control were successfully mapped to this bearer, the reception by the MCPTT client can continue (until UnmapGroupToBearer is received or until timeout) throughout the entire MBMS service area of this bearer.

e) may include the <report-suspension> element and set it to "true" value or the "false" value; and

NOTE 8: The participating function can choose to direct some clients not to send an MBMS bearer suspension report when notified by RAN, by including the <report-suspension> element set to "false". The purpose is to prevent an avalanche of identical reports sent by clients roughly at the same time, to report the suspension of the same MBMS bearer. The way the participation function determines which clients are to send or not to send the report is outside the scope of the present document.

f) if the MBMS bearer is carrying the general purpose MBMS subchannel, shall include one <GPMS>element, giving the number of the "m=application" media line in the application/sdp MIME body generated in step 5 above to be used for the general purpose MBMS subchannel;

7) shall include the MBMS public service identity of the participating MCPTT function in the P-Asserted-Identity header field;

8) shall include in a MIME body with Content-Type header field set to "application/vnd.3gpp.mcptt-info+xml", the <mcptt-request-uri> element set to the MCPTT ID of the user; and

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

14.2.2.3 Updating an announcement

When the participating MCPTT function wants to update a previously sent announcement, the participating MCPTT function sends an MBMS bearer announcement in an SIP MESSAGE request as specified in subclause 14.2.2.2 where the participating MCPTT function in the <announcement> element to be updated:

1) shall include the same TMGI value as in the MBMS bearer announcement to be updated in the <TMGI> element;

NOTE 1: TMGI value is used to identify the <announcement> when updating or cancelling the <announcement> element and can't be changed.

2) shall include the same or an updated value of the QCI in the <QCI> element;

3) if a frequency was included in the previously sent announcement, shall include the same value in the <frequency> element;

NOTE 2: In the current release if the <frequency> element is included, the frequency in the <frequency> element is the same as the frequency used for unicast.

4) shall include the same list of MBMS service area IDs or an updated list of MBMS service area IDs in the <mbms-service-areas> element;

5) may include the same or an updated value in the <report-suspension> element;

6) shall include the <GPMS> element with the same value as in the initial <announcement> element; and

7) shall include the same application/sdp MIME body as included in the initial MBMS announcement.

14.2.2.4 Cancelling an MBMS bearer announcement

When the participating MCPTT function wants to cancel an MBMS bearer announcement associated with an <announcement> element, the participating MCPTT function sends an MBMS bearer announcement as specified in subclause 14.2.2.2 where the participating MCPTT function in the <announcement> element to be cancelled:

1) shall include the same TMGI value as in the <announcement> element to be cancelled in the <TMGI> element;

2) shall not include an <mbms-service-areas> element;

3) if the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body only contains <announcement> elements that are to be cancelled, shall not include an <GPMS> element; and

4) if the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body only contains <announcement> elements that are to be cancelled, shall not include an application/sdp MIME body.

14.2.2.5 Sending a MuSiK download message

For each MCPTT client that the participating MCPTT function is intending to use an MBMS bearer to transmit confidentiality protected floor control signalling (SRTCP) to the client, the participating MCPTT function shall perform a key download procedure for each Multicast Siganlling Key (MuSiK). Two kinds of MuSiK download are possible: default MuSiK download and explicit MuSiK download. The default MuSiK download is used to set, reset or unset a MuSiK and its corresponding MuSiK-ID and is applicable to all groups supported by the MCPTT client, except for certain identified groups for which MuSiKs and MUSiK-IDs are assigned, reassigned or unassigned separately via explicit MuSiK download. The default MuSiK and MUSiK-ID can apply to all the MCPTT clients supported by the participating MCPTT function and can be overridden by the explicit MuSiK download which is selectively applied only to the MCPTT clients using the explicitly identified groups. A group subject to explicit MuSiK download, can be switched to the default MuSiK protection via a default MuSiK download identifying that group. The participating MCPTT function:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33];

2) shall set the Request-URI to the URI received in the To header field in a third-party SIP REGISTER request;

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

4) shall include a P-Asserted-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

5) shall include an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body defined in subclause F.2 with the <version> element set to "1", and either

   a) containing an <mbms-explicitMuSiK-download> element with at least one <group> element associated with the MuSiK being downloaded; or

   b) containing an <mbms-defaultMuSiK-download> element with zero or more <group> elements associated with the MuSiK being downloaded;

6) if the floor control signaling for the group(s) in the specified list is to be protected using the MuSiK, shall include an application/mikey MIME body with the MIKEY message containing the encrypted MuSiK and the corresponding MuSiK-ID, constructed as described in subclauses 5.8.1 and 5.2.2 of 3GPP TS 33.180 [78];

NOTE: Subclause 9.2.1.3 of 3GPP TS 33.180 [78] shows an example on how to include an application/mikey MIME body in a SIP message.

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

The participating MCPTT function shall consider the key download successful on receipt of a 200 OK message in response to the SIP MESSAGE request sent in step 7).

A participating MCPTT function that does not receive a 200 OK message from a specific MCPTT client shall use unicast signalling for floor control towards that MCPTT client for the groups for which the MuSiK was intended.

14.2.3 Receiving an MBMS bearer listening status from an MCPTT client

Upon receiving a "SIP MESSAGE request for an MBMS listening status update", the participating MCPTT function shall handle the request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33].

If the SIP MESSAGE request contains:

1) an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body with an <mbms-listening-status> element; and

2) an application/vnd.3gpp.mcptt-info+xml MIME body containing an MCPTT ID in the <mcptt-request-uri> served by the participating MCPTT function;

then the participating MCPTT function:

1) shall verify that the public user identity in the P-Asserted-Identity header field is bound to the MCPTT ID in the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body, and if that is the case:

   a) if the <mbms-listening-status> element is set to "listening":

      i) if <session-identifier> elements are included, shall indicate to the media plane that the MCPTT client in the session identified by the <session-identifier> element is now listening to the MBMS subchannel; and

      ii) if <general-purpose> element is included with the value "true", shall indicate to the media plane that the MCPTT client is now listening to the general purpose MBMS subchannel; and

   b) if the <mbms-listening-status> element is set to "not-listening":

      i) if <session-identifier> elements are included, shall indicate to the media plane that the MCPTT client in the sessions identified by the <session-identifier> elements is not listening to the MBMS subchannel;

      ii) if <general-purpose> element is included with the value "false", shall indicate to the media plane that the MCPTT client is no longer listening to the general purpose MBMS bearer; and

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

NOTE 1: If the MCPTT client reports that the MCPTT client is no longer listening to the general purpose MBMS subchannel it is implicitly understood that the MCPTT client no longer listens to any MBMS subchannel in ongoing conversations that the MCPTT client previously reported status "listening".

If the SIP MESSAGE request contains:

1) an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body with an <mbms-suspension-status> element; and

2) an application/vnd.3gpp.mcptt-info+xml MIME body containing an MCPTT ID in the <mcptt-request-uri> served by the participating MCPTT function;

then the participating MCPTT function:

1) shall verify that the public user identity in the P-Asserted-Identity header field is bound to the MCPTT ID in the <mcptt-request-uri> element in the application/vnd.3gpp.mcptt-info+xml MIME body, and if that is the case:

   a) if the <mbms-suspension-status> element is set to "suspending":

      i) shall consider that the bearer identified by the <suspended-TMGI> element is about to be suspended and that the reduction or elimination of traffic on that bearer and/or on some of the bearers indicated in the <other-TMGI> elements can potentially avoid the suspension; and

NOTE 2: An MBMS bearer is about to be suspended when RAN has notified the clients of the decision to suspend the bearer, but the actual suspension, which would occur at the end of the MCCH modification period, has not taken place yet because the MCCH modification period has not yet expired.

      ii) may take implementation/configuration specific immediate action for the MCPTT client that reports the suspension as well as other MCPTT clients that listen to the same bearer (e.g. moving traffic to unicast bearer(s)), reducing transmission rate, eliminating traffic, modifying pre-emption priority).

   b) if the <mbms-suspension-status> element is set to "not-suspending":

      i) shall consider that the bearer identified by the <suspended-TMGI> element is no longer about to be suspended; and

NOTE 3: An MBMS bearer is no longer about to be suspended when RAN has notified the clients of the decision to no longer suspend the bearer after having previously notified the clients that the bearer would be suspended at the end of the MCCH modification period. The RAN notifications to first suspend and subsequently not to suspend the same MBMS bearer would have to come within the same MCCH modification period.

      ii) may take implementation/configuration specific immediate action for the MCPTT client that reports the suspension as well as other MCPTT clients that listen to the same bearer (e.g. restoring traffic previously reduced or eliminated from MBMS bearers upon reception of suspension information).

NOTE 4: If the MCPTT client reports that the MCPTT client is no longer listening to MBMS subchannels associated with the MBMS bearer indicated in the suspension information, it is implicitly understood that the suspension of that MBMS bearer has actually occurred.

14.2.4 Abnormal cases

Upon receipt of a SIP MESSAGE request with an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body:

1) where the P-Asserted-Identity identifies a public user identity not associated with MCPTT user served by the participating MCPTT function; or

2) with an application/vnd.3gpp.mcptt-info+xml MIME body and with a <mcptt-request-uri> element containing an MCPTT ID that identifies an MCPTT user served by the participating MCPTT function and an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body containing one or more <announcement> elements;

then the participating MCPTT function shall send a SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [4].

14.3 MCPTT client MBMS usage procedures

14.3.1 General

This subclause describes the procedures in the MCPTT client for:

1) receiving an MBMS bearer announcement from the participating MCPTT function;

2) sending an MBMS bearer listening status report to the participating MCPTT function; and

3) sending an MBMS bearer suspension status report to the participating MCPTT function.

14.3.2 Receiving an MBMS bearer announcement

The MCPTT client associates each received application/sdp MIME body and each received security key with a general purpose MBMS subchannel announced in the same MBMS Bearer Announcement message. When receiving a MapGroupToBearer message, the MCPTT client interprets its content (e.g. the m= line number) in the context of the application/sdp MIME body associated with the general purpose MBMS subchannel on which the MapGroupToBearer was received.

When the MCPTT client receives a SIP MESSAGE request containing:

1) a P-Asserted-Service header field containing the "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

2) an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body containing one or more an <announcement> element(s);

then the MCPTT client for each <announcement> element in the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body:

1) if the <mbms-service-areas> element is present and contains at least one MBMS service area ID:

   a) if an <announcement> element with the same value of the <TMGI> element is already stored:

      i) shall replace the old <announcement> element with the <announcement> element received in the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body;

   b) if there is no <announcement> element with the same value of the <TMGI> element stored:

      i) shall store the received <announcement> element;

   c) shall associate the received announcement with the received application/sdp MIME body;

   d) shall associate the received announcement with the received <GPMS> element;

   e) shall store the MBMS public service identity of the participating MCPTT function received in the P-Asserted-Identity header field and associate the MBMS public service identity with the new <announcement> element;

   f) if a "a=key-mgmt" media-level attribute with the "mikey" key management and protocol identifier and a MIKEY-SAKKE I_MESSAGE is included for the general purpose MBMS subchannel defined in the "m=application" media line in the application/sdp MIME body in the received SIP MESSAGE request,

      i) shall extract the initiator URI from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.179 [46]. If the initiator URI deviates from the public service identity of the participating MCPTT function serving the MCPTT user, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and include warning text set to "136 authentication of the MIKEY-SAKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

      ii) shall convert the initiator URI to a UID as described in 3GPP TS 33.179 [46];

      iii) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.179 [46];

iv) if authentication verification of the MIKEY-SAKKE I_MESSAGE fails, shall reject the SIP MESSAGE request with a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and include warning text set to "136 authentication of the MIKEY-SAKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

v) shall extract and decrypt the encapsulated MSCCK using the participating MCPTT function's (KMS provisioned) UID key as described in 3GPP TS 33.179 [46]; and

vi) shall extract the MSCCK-ID, from the payload as specified in 3GPP TS 33.179 [46];

NOTE: With the MSCCK successfully shared between the participating MCPTT function and the served UEs, the participating MCPTT function is able to securely send MBMS subchannel control messages to the MCPTT clients.

g) shall listen to the general purpose MBMS subchannel defined in the "m=application" media line in the application/sdp MIME body in the received SIP MESSAGE request when entering an MBMS service area where the announced MBMS bearer is available; and

h) shall check the condition for sending a listening status report as specified in the subclause 14.3.3; and

2) if no <mbms-service-areas> element is present:

a) shall discard a previously stored <announcement> element identified by the value of the <TMGI>;

b) shall remove the association with the stored application/sdp MIME body and stop listening to the general purpose MBMS subchannel;

c) if no more <announcement> elements associated with the stored application/sdp MIME body are stored in the MCPTT client, shall remove the stored application/sdp MIME body; and

d) check the condition for sending a listening status report as specified in the subclause 14.3.3.

14.3.3 The MBMS bearer listening status and suspension report procedures

14.3.3.1 Conditions for sending an MBMS listening status report

If one of the following conditions is fulfilled:

1) if the MCPTT client:

a) receives a Map Group To Bearer message over the general purpose MBMS channel;

b) participates in a group session identified by the Map Group To Bearer message; and

c) the status "listening" is not already reported; or

2) if the MCPTT client:

a) receives an announcement as described in subclause 14.3.2;

b) enters an MBMS service area where a general purpose MBMS is available; and

c) experiences good MBMS bearer radio condition;

then the MCPTT client shall report that the MCPTT client is listening to the MBMS bearer as specified in subclause 14.3.3.2.

If one of the following conditions is fulfilled:

1) if the MCPTT client:

a) receives an MBMS bearer announcement as described in the subclause 14.3.2;

b) the MBMS bearer announcement contains a cancellation of an <announcement> element identified by the same TGMI value as received in a Map Group To Bearer message in an ongoing conversation; and

c) the status "not-listening" is not already reported;

2) if the MCPTT client:

a) receives an MBMS bearer announcement as described in the subclause 14.3.2;

b) the MBMS bearer announcement contains a cancellation of an <announcement> element;

c) does not participate in an ongoing conversation;

d) the MCPTT client has reported the "listening" status due to the availability of the general purpose MBMS subchannel in the <announcement> element; and

e) the status "not-listening" is not already reported; or

3. if the MCPTT client:

a) suffers from bad MBMS bearer radio condition,

then the MCPTT client shall report that the MCPTT client is not listening to the MBMS subchannels as specified in subclause 14.3.3.2.

If all the following conditions are fulfilled:

1) the MCPTT client has reported "listening" as the most recent listening status relative to an MBMS bearer;

2) the MCPTT client is notified that the MBMS bearer is about to be suspended by the RAN; and

3) the MCPTT client has not received a MBMS bearer announcement containing a <report-suspension> element set to "false",

then the MCPTT client shall report that the MBMS bearer is about to be suspended, as specified in subclause 14.3.3.2.

If all the following conditions are fulfilled:

1) the MCPTT client has reported "listening" as the most recent listening status relative to an MBMS bearer;

2) the MCPTT client has reported that the MBMS bearer is about to be suspended, but the suspension of the bearer has not been detected yet by the MCPTT client;

3) the MCPTT client is notified that the MBMS bearer is no longer to be suspended by the RAN; and

4) the MCPTT client has not received a MBMS bearer announcement containing a <report-suspension> element set to "false",

then the MCPTT client shall report that the MBMS bearer is no longer to be suspended, as specified in subclause 14.3.3.2.

14.3.3.2 Sending the MBMS bearer listening or suspension status report

When the MCPTT client wants to report the MBMS bearer listening status, the MCPTT client:

NOTE 1: The application/vnd.3gpp.mcptt-mbms-usage-info+xml can contain both the listening status "listening" and "not listening" at the same time.

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33]; and

2) the SIP MESSAGE request:

a) shall include in the Request-URI the MBMS public service identity of the participating MCPTT function received in the P-Asserted-Identity header field of the announcement message;

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

c) should include a public user identity in the P-Preferred-Identity header field as specified in 3GPP TS 24.229 [4];

d) shall include a P-Preferred-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

e) shall include an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body with the <version> element set to "1";

f) if the MCPTT client is listening to the MBMS bearer, the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body:

i) shall include an <mbms-listening-status> element set to "listening";

ii) if the intention is to report that the MCPTT client is listening to the MBMS subchannel for an ongoing conversation in a session (e.g. as the response to the Map Group To Bearer message), shall include the MCPTT session identity of the ongoing conversation in <session-identity> element;

iii) shall include one or more <TGMI> elements for which the listening status applies; and

iv) if the intention is to report that the MCPTT client is listening to the general purpose MBMS subchannel, shall include the <general-purpose> element set to "true";

g) if the MCPTT client is not listening, the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body:

i) shall include an <mbms-listening-status> element set to "not-listening";

iii) shall include one or more <TGMI> elements for which the listening status applies;

iii) if the intention is to report that the MCPTT client is no longer listening to the MBMS subchannel in an ongoing session (e.g. as the response to Unmap Group to Bearer message), shall include the MCPTT session identity in <session-identity> elements; and

iv) if the intention is to report that the MCPTT client is no longer listening to general purpose MBMS subchannel, shall include the <general-purpose> element set to "false"; and

NOTE 2: If the MCPTT client reports that the MCPTT client is no longer listening to the general purpose MBMS subchannel, it is implicitly understood that the MCPTT client no longer listens to any MBMS subchannel in ongoing conversations that the MCPTT client previously reported status "listening".

h) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcptt-request-uri> set to the MCPTT ID; and

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

When the MCPTT client meets all the conditions specified in subclause 14.3.3.1 for reporting a change in an MBMS bearer suspension status, the MCPTT client:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [4] and IETF RFC 3428 [33]; and

2) the SIP MESSAGE request:

a) shall include in the Request-URI the MBMS public service identity of the participating MCPTT function received in the P-Asserted-Identity header field of the announcement message;

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

c) should include a public user identity in the P-Preferred-Identity header field as specified in 3GPP TS 24.229 [4];

d) shall include a P-Preferred-Service header field with the value "urn:urn-7:3gpp-service.ims.icsi.mcptt";

e) shall include an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body with the <version> element set to "1";

f) if at least one MBMS bearer is about to be suspended, the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body:

i) shall include an <mbms-suspension-status> element set to "suspending";

ii) shall set the <number-of-reported-bearers> element to the total number of the included <supended-TMGI> elements and <other-TMGI> elements;

iii) shall include <suspended-TMGI> element(s) set to the TMGI value for each of the MTCHs on the same MCH corresponding to the MBMS bearers about to be supended; and

iv) may include <other-TMGI> elements, if available, corresponding to the TMGI values for other MTCHs on the same MCH as the MBMS bearers to be suspended

NOTE 3: To report the suspension of MTCHs on different MCHs, the MCPTT client sends a separate message for each of the involved MCHs.

g) if the MBMS bearer is no longer about to be suspended, the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body:

i) shall include an <mbms-suspension-status> element set to "not-suspending";

ii) shall set the <number-of-reported-bearers> element to the number of included <suspended-TMGI> elements; and

iii) shall include a <suspended-TMGI> element set to the corresponding TMGI value for each of the MTCHs of the MBMS bearers that are no longer about to be suspended; and

h) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with the <mcptt-request-uri> set to the MCPTT ID; and

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

NOTE 4: The MCPTT client reports in separate messages the MBMS bearers that are about to be suspended and the MBMS bearers that are no longer about to be suspended.

14.3.4 Receiving a MuSiK download message

When the MCPTT client receives a SIP MESSAGE request containing:

1) a P-Asserted-Service header field containing the "urn:urn-7:3gpp-service.ims.icsi.mcptt"; and

2) with one of the following:

a) an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body containing an <mbms-explicitMuSiK-download> element with at least one <group> subelement; or

b) an application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body containing an <mbms-defaultMuSiK-download> element with zero or more <group> subelements;

the MCPTT client shall:

1) if the received message contains an <mbms-explicitMuSiK-download> element, set the impacted groups to be those groups identified by the <group> subelements;

2) if the received message contains an <mbms-defaultMuSiK-download> element without <group> subelements, set the impacted groups to be all groups not associated with currently valid explicit MuSiK downloads; and

3) if the received message contains an <mbms-defaultMuSiK-download> element with <group> subelements, first dissociate those groups identified by the <group> subelements from currently valid associations with explicit MuSiK downloads and then set the impacted groups to be all groups not associated with currently valid explicit MuSiK downloads.

If the key identifier within the CSB-ID of the MIKEY payload is a MuSiK-ID (4 most-significant bits have the value '6'), the MCPTT client:

1) shall process the MIKEY payload according to 3GPP TS 33.180 [78], as follows:

   a) if the initiator field (IDRi) has type 'URI' (identity hiding is not used), the client:

      i) shall extract the initiator URI from the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]. If the initiator URI deviates from the public service identity of the participating MCPTT function serving the MCPTT client, shall reject the SIP MESSAGE request by sending a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and including warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps; and

      ii) shall convert the initiator URI to a UID as described in 3GPP TS 33.180 [78];

   b) otherwise, if the initiator field (IDRi) has type 'UID' (identity hiding in use), the client:

      i) shall convert the public service identity of participating MCPTT function serving the MCPTT user to a UID as described in 3GPP TS 33.180 [78]; and

      ii) shall compare the generated UID with the UID in the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [78]. If the two initiator UIDs deviate from each other, shall reject the SIP MESSAGE request by sending a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and including warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

   c) otherwise, shall reject the SIP MESSAGE request by sending a SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and including warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps;

   d) shall use the UID to validate the signature of the I_MESSAGE as described in 3GPP TS 33.180 [78];

   e) if authentication verification of the I_MESSAGE fails or the I_MESSAGE does not contain a Status attribute, shall reject the SIP MESSAGE request by sending SIP 488 (Not Acceptable Here) response as specified in IETF RFC 4567 [47], and including warning text set to "136 authentication of the MIKEY-SAKKE I_MESSAGE failed" in a Warning header field as specified in subclause 4.4 and shall not continue with the rest of the steps; and

   f) shall examine the Status attribute and shall either mark the associated security functions as "not in use" or shall extract and store the encapsulated MuSiK and the corresponding MuSiK-ID from the payload as specified in 3GPP TS 33.180 [78]; and

2) for each of the impacted groups, shall either associate the status 'security not in use' or shall add/replace in the storage associated with the group the MuSiK-ID and the MuSiK, for use (decrypted) as security key for floor control.

NOTE: It is expected that the MCPTT client is capable of storing a different MuSiK for each MCPTT group of interest.

The MCPTT client shall respond with SIP 200 OK only if it finds the message syntactically correct and recognizes it as a valid and error-free MuSiK download (default or explicit) message.

14A MCPTT Service Continuity

14A.1 General

This clause describes the procedures for service continuity of an ongoing SIP session supporting an MCPTT private call or MCPTT group call when:

- the MCPTT UE (referred to as the remote UE) is connected to the network via E-UTRAN and decides to connect to a UE-to-network relay, e.g. because it realises that it is losing connection to the network and wants to ensure seamless service; and

- the remote UE is connected to the network via the UE-to-network-relay and decides to disconnect from the UE-to-network relay, e.g. because the remote UE realises that it is losing connection to UE-to-network relay or because the LTE-Uu link quality goes above a certain threshold, and decides to connect to the network via E-UTRAN for seamless service.

MCPTT service continuity follows the principles of 3GPP TS 24.237 [58] for PS-PS service continuity. In particular:

1) the SIP session is anchored at a Service Centralisation and Continuity Application Server (SCC AS) before and after the handover. This requires that initial filter criteria is configured to ensure that the SCC AS is in the registration path, is the first application server in the path of an originating session, and the last AS in the path of a terminating session;

2) the remote UE is an SC UE that supports PS-PS access transfer as per 3GPP TS 24.237 [58]; and

3) the remote UE is either configured with a static PS to PS STI as specified in 3GPP TS 24.216 [66] that it uses when initiating the session transfer request, or it uses a dynamic PS to PS STI which is the URI contained in the Contact header field returned at the creation of the dialog over the Source Access Leg, as specified in 3GPP TS 24.237 [58].

14A.2 Service continuity from on-network MCPTT service to UE-to-network relay MCPTT service

14A.2.1 Remote UE

When performing service continuity from on-network MCPTT service to UE-to-network relay MCPTT service, the remote UE:

1) shall perform ProSe UE-to-network relay discovery over PC5 as specified in clause 10A of 3GPP TS 24.334 [28];

NOTE 1: Depending on the model (A or B) used for discovery as specified in 3GPP TS 24.334 [28], the remote UE can perform UE-to-network relay discovery while still in coverage (when model A is used), or while still in coverage if the LTE-Uu link quality drops below a certain threshold (when model B is used).

NOTE 2: As part of the discovery process, service authorisation is performed as specified in 3GPP TS 24.334 [28]. The UE-to-network relay is provisioned with relay service code(s) associated with allowed MCPTT group(s) as specified in 3GPP TS 24.483 [45] and 3GPP TS 24.484 [50]. To find a permitted UE-to-network relay for group communications, a remote UE is provisioned with the relay service code(s) associated with the MCPTT group(s) which the MCPTT user is part of, in the MCPTT group configuration MO as specified in 3GPP TS 24.483 [45].

2) shall select a suitable UE-to-network relay by performing the UE-to-network relay selection procedure specified in subclause 10A.2.12 of 3GPP TS 24.334 [28];3) shall establish a direct link to the relay as specified in subclause 10.4.2 of 3GPP TS 24.334 [28];

NOTE 3: As part of this process the remote UE is assigned a /64 IPv6 Prefix by the relay.

4) shall initiate IMS registration over the UE-to-network relay target access leg by following the procedures in subclause 10.2.0 of 3GPP TS 24.237 [58];

NOTE 4: As part of this process the remote UE needs to discover the P-CSCF address to connect to via the UE-to-network relay. The remote UE either uses mechanism I or mechanism III of subclause 9.2.1 in 3GPP TS 24.229 [4] to discover the P-CSCF address. The details of how mechanism I or mechanism III are used to discover the P-CSCF address are not covered by the present document.

5) shall initiate session transfer by following the procedures specified in subclause 10.2.1 of 3GPP TS 24.237 [58];

6) after successful session transfer if MCPTT content is being distributed on the target side using MBMS bearers, shall send a MBMS bearer listening status report procedure to the participating MCPTT function by performing the procedures in subclause 14.3.3; and

NOTE 5: Upon receiving the MBMS bearer listening status from an MCPTT client indicating that the MCPTT UE is now listening to a MBMS subchannel, the participating MCPTT function performs the procedures in subclause 14.2.3 to switch to MBMS bearer.

7) after successful session transfer if the remote UE still has an connection in the source access, may perform IMS de-registration of the contact address of the IMS public user identity registered on the source access leg by following the procedures in 3GPP TS 24.229 [4];

14A.2.2 SCC AS

The SCC AS follows the procedures in subclause 10.3.2 of 3GPP TS 24.237 [58].

14A.3 Service continuity from UE-to-network relay MCPTT service to on-network MCPTT service

14A.3.1 Remote UE

When performing access transfer between UE-to-network relay MCPTT service and on-network MCPTT service, the remote UE:

1) shall initiate IMS registration over the on-network target access leg by following the procedures in subclause 10.2.0 of 3GPP TS 24.237 [58]; and

NOTE: The remote UE uses option II procedures for P-CSCF discovery as defined in subclause L.2.2.1 of 3GPP TS 24.229 [4] to discover the P-CSCF address when connecting to EPC.

2) follows the procedures in steps 5), 6) and 7) of subclause 14.A.2.1.

14A.3.2 SCC AS

The SCC AS follows the procedures in subclause 14A.2.2.

15 Off-network message formats

15.1 MONP message functional definitions and contents

15.1.1 General

The following subclauses describe the MONP message functional definitions and contents. Each message consist of a series of information elements. Annex I describes the standard format of a MONP message and the encoding rules for each type of information element.

15.1.2 GROUP CALL PROBE message

15.1.2.1 Message definition

This message is sent by the UE to other UEs to check for an ongoing group call. For contents of the message see Table 15.1.2.1-1.

Message type: GROUP CALL PROBE

Direction: UE to other UEs

Table 15.1.2.1-1: GROUP CALL PROBE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group call probe message identity	Message type 15.2.2	M	V	1
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x

15.1.3 GROUP CALL ANNOUNCEMENT message

15.1.3.1 Message definition

This message is sent by the UE to other UEs to announce an ongoing group call to other UEs. For contents of the message see Table 15.1.3.1-1.

Message type: GROUP CALL ANNOUNCEMENT

Direction: UE to other UEs

Table 15.1.3.1-1: GROUP CALL ANNOUNCEMENT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group call announcement message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	Call type	Call type 15.2.11	M	V	1
	Refresh interval	Refresh interval 15.2.4	M	V	2
	Call start time	Call start time 15.2.14	M	V	5
	Last call type change time	Last call type change time 15.2.15	M	V	5
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	SDP	SDP 15.2.6	M	LV-E	3-x
	Originating MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x
	Last user to change call type	MCPTT User ID 15.2.10	M	LV-E	3-x
80	Confirm mode indication	Confirm mode indication 15.2.9	O	T	1
81	Probe response	Probe response 15.2.16	O	T	1

15.1.4 GROUP CALL ACCEPT message

15.1.4.1 Message definition

This message is sent by the UE to other UEs to indicate acceptance of a group call. For contents of the message see Table 15.1.4.1-1.

Message type: GROUP CALL ACCEPT

Direction: UE to other UEs

Table 15.1.4.1-1: GROUP CALL ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group call accept message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	Call type	Call type 15.2.11	M	V	1
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	Sending MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.5 PRIVATE CALL SETUP REQUEST message

15.1.5.1 Message definition

This message is sent by a UE to another UE to request setup of a private call. For contents of the message see Table 15.1.5.1-1.

Message type: PRIVATE CALL SETUP REQUEST

Direction: UE to another UE

Table 15.1.5.1-1: PRIVATE CALL SETUP REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call setup request message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	Commencement mode	Commencement mode 15.2.7	M	V	1
	Call type	Call type 15.2.11	M	V	1
	MCPTT user ID of the caller	MCPTT user ID 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user ID 15.2.10	M	LV-E	3-x
	SDP offer	SDP 15.2.6	M	LV-E	3-x
78	User location	User location 15.2.12	O	TLV-E	4-x

15.1.6 PRIVATE CALL RINGING message

15.1.6.1 Message definition

This message is automatically sent by a UE to another UE in response to a PRIVATE CALL SETUP REQUEST message. This message indicates that the UE has presented the incoming call notification to the user and is awaiting user response. For contents of the message see Table 15.1.6.1-1.

Message type: PRIVATE CALL RINGING

Direction: UE to another UE

Table 15.1.6.1-1: PRIVATE CALL RINGING message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call ringing message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	MCPTT user ID of the caller	MCPTT user ID 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.7 PRIVATE CALL ACCEPT message

15.1.7.1 Message definition

This message is sent by a UE to another UE in response to a PRIVATE CALL SETUP REQUEST message when user accepts the call. This message indicates that the UE accepts the call setup request. For contents of the message see Table 15.1.7.1-1.

Message type: PRIVATE CALL ACCEPT

Direction: UE to another UE

Table 15.1.7.1-1: PRIVATE CALL ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call accept message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	MCPTT user ID of the caller	MCPTT user ID 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user ID 15.2.10	M	LV-E	3-x
	SDP answer	SDP 15.2.6	M	LV-E	3-x

15.1.8 PRIVATE CALL REJECT message

15.1.8.1 Message definition

This message is sent by a UE to another UE in response to a PRIVATE CALL SETUP REQUEST message when user rejects the call. This message indicates that the UE rejects the call setup request. For contents of the message see Table 15.1.8.1-1.

Message type: PRIVATE CALL REJECT

Direction: UE to another UE

Table 15.1.8.1-1: PRIVATE CALL REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call reject message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	Reason	Reason 15.2.8	M	V	1
	MCPTT user ID of the caller	MCPTT user ID 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.9 PRIVATE CALL RELEASE message

15.1.9.1 Message definition

This message is sent by a UE to another UE to terminate an ongoing private call. For contents of the message see Table 15.1.9.1-1.

Message type: PRIVATE CALL RELEASE

Direction: UE to another UE

Table 15.1.9.1-1: PRIVATE CALL RELEASE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call release message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	MCPTT user ID of the caller	MCPTT user id 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user id 15.2.10	M	LV-E	3-x

15.1.10 PRIVATE CALL RELEASE ACK message

15.1.10.1 Message definition

This message is sent by a UE to another UE in response to a PRIVATE CALL RELEASE message. This message indicates that the UE has terminated the call. For contents of the message see Table 15.1.10.1-1.

Message type: PRIVATE CALL RELEASE ACK

Direction: UE to another UE

Table 15.1.10.1-1: PRIVATE CALL RELEASE ACK message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call release ack message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	MCPTT user ID of the caller	MCPTT user id 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.11 PRIVATE CALL ACCEPT ACK message

15.1.11.1 Message definition

This message is sent by a UE to another UE in response to a PRIVATE CALL ACCEPT message. This message acknowledges the receipt of PRIVATE CALL ACCEPT message. For contents of the message see Table 15.1.11.1-1.

Message type: PRIVATE CALL ACCEPT ACK

Direction: UE to another UE

Table 15.1.11.1-1: PRIVATE CALL ACCEPT ACK message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call accept ack message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	MCPTT user ID of the caller	MCPTT user ID 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.12 PRIVATE CALL EMERGENCY CANCEL message

15.1.12.1 Message definition

This message is sent by a UE to another UE to indicate termination of emergency mode in private call. For contents of the message see Table 15.1.12.1-1.

Message type: PRIVATE CALL EMERGENCY CANCEL

Direction: UE to another UE

Table 15.1.12.1-1: PRIVATE CALL EMERGENCY CANCEL message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call emergency cancel message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	MCPTT user ID of the caller	MCPTT user ID 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.13 PRIVATE CALL EMERGENCY CANCEL ACK message

15.1.13.1 Message definition

This message is sent by a UE to another UE to indicate receipt of PRIVATE CALL EMERGENCY CANCEL message. For contents of the message see Table 15.1.13.1-1.

Message type: PRIVATE CALL EMERGENCY CANCEL ACK

Direction: UE to another UE

Table 15.1.13.1-1: PRIVATE CALL EMERGENCY CANCEL ACK message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Private call emergency cancel ack message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	MCPTT user ID of the caller	MCPTT user ID 15.2.10	M	LV-E	3-x
	MCPTT user ID of the callee	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.14 GROUP CALL IMMINENT PERIL END message

15.1.14.1 Message definition

This message is sent by the UE to other UEs to indicate termination of imminent peril mode in the group call. For contents of the message see Table 15.1.14.1-1.

Message type: GROUP CALL IMMINENT PERIL END

Direction: UE to other UEs

Table 15.1.14.1-1: GROUP CALL IMMINENT PERIL END message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group call imminent peril end message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	Last call type change time	Last call type change time 15.2.16	M	V	5
	Last user to change call type	MCPTT User ID 15.2.10	M	LV-E	3-x
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	Originating MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.15 GROUP CALL EMERGENCY END message

15.1.15.1 Message definition

This message is sent by the UE to other UEs to indicate termination of emergency mode in the group call. For contents of the message see Table 15.1.15.1-1.

Message type: GROUP CALL EMERGENCY END

Direction: UE to other UEs

Table 15.1.15.1-1: GROUP CALL EMERGENCY END message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group call emergency end message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	Last call type change time	Last call type change time 15.2.16	M	V	5
	Last user to change call type	MCPTT User ID 15.2.10	M	LV-E	3-x
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	Originating MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.16 GROUP EMERGENCY ALERT message

15.1.16.1 Message definition

This message is sent by the UE to other UEs to indicate an emergency situation. For contents of the message see Table 15.1.16.1-1.

Message type: GROUP EMERGENCY ALERT

Direction: UE to other UEs

Table 15.1.16.1-1: GROUP EMERGENCY ALERT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group emergency alert message identity	Message type 15.2.2	M	V	1
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	Originating MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x
	Organization name	Organization name 15.2.13	M	LV-E	3-x
78	User location	User location 15.2.12	O	TLV-E	4-x

15.1.17 GROUP EMERGENCY ALERT ACK message

15.1.17.1 Message definition

This message is sent by the UE to other UEs to indicate receipt of emergency alert. For contents of the message see Table 15.1.17.1-1.

Message type: GROUP EMERGENCY ALERT ACK

Direction: UE to other UEs

Table 15.1.17.1-1: GROUP EMERGENCY ALERT ACK message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group emergency alert ack message identity	Message type 15.2.2	M	V	1
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	Originating MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x
	Sending MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.18 GROUP EMERGENCY ALERT CANCEL message

15.1.18.1 Message definition

This message is sent by the UE to other UEs to indicate end of emergency situation. For contents of the message see Table 15.1.18.1-1.

Message type: GROUP EMERGENCY ALERT CANCEL

Direction: UE to other UEs

Table 15.1.18.1-1: GROUP EMERGENCY ALERT CANCEL message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group emergency alert cancel 0message identity	Message type 15.2.2	M	V	1
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	Originating MCPTT user ID	MCPTT User ID 15.2.10	M	LV-E	3-x
	Sending MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.19 GROUP EMERGENCY ALERT CANCEL ACK message

15.1.19.1 Message definition

This message is sent by the UE to other UEs to indicate receipt of emergency alert cancel. For contents of the message see Table 15.1.19.1-1.

Message type: GROUP EMERGENCY ALERT CANCEL ACK

Direction: UE to other UEs

Table 15.1.19.1-1: GROUP EMERGENCY ALERT CANCEL ACK message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group emergency alert cancel ack message identity	Message type 15.2.2	M	V	1
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	Originating MCPTT user ID	MCPTT User ID 15.2.10	M	LV-E	3-x
	Sending MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x

15.1.20 GROUP CALL BROADCAST message

15.1.20.1 Message definition

This message is sent by the UE to other UEs to announce a broadcast group call to other UEs. For contents of the message see Table 15.1.20.1-1.

Message type: GROUP CALL BROADCAST

Direction: UE to other UEs

Table 15.1.20.1-1: GROUP CALL BROADCAST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group call broadcast message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	Call type	Call type 15.2.11	M	V	1
	Originating MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x
	MCPTT group ID	Group ID 15.2.5	M	LV-E	3-x
	SDP	SDP 15.2.6	M	LV-E	3-x

15.1.21 GROUP CALL BROADCAST END message

15.1.21.1 Message definition

This message is sent by the UE to other UEs to indicate termination of a broadcast group call. For contents of the message see Table 15.1.21.1-1.

Message type: GROUP CALL BROADCAST END

Direction: UE to other UEs

Table 15.1.21.1-1: GROUP CALL BROADCAST END message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Group call broadcast end message identity	Message type 15.2.2	M	V	1
	Call identifier	Call identifier 15.2.3	M	V	2
	MCPTT group ID	MCPTT group ID 15.2.5	M	LV-E	3-x
	Originating MCPTT user ID	MCPTT user ID 15.2.10	M	LV-E	3-x

15.2 General message format and information elements coding

15.2.1 General

The least significant bit of a field is represented by the lowest numbered bit of the highest numbered octet of the field. When the field extends over more than one octet, the order of bit values progressively decreases as the octet number increases.

Figure 15.2.1-1 shows an example of a field where the most significant bit of the field is marked MSB and the least significant bit of the field is marked LSB.

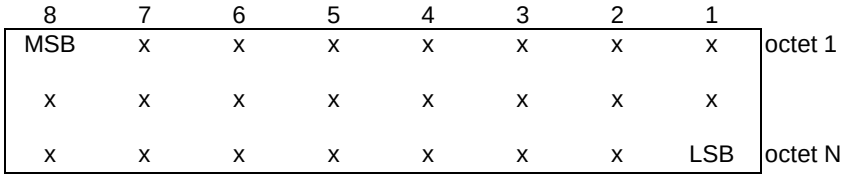

Figure 15.2.1-1: Example of bit ordering of a field

Within the protocols defined in the present document, the message consists of the following parts:

a) message type information element; and

b) other information elements, as required.

The organization of a message is illustrated in the example shown in Figure 15.2.1-2.

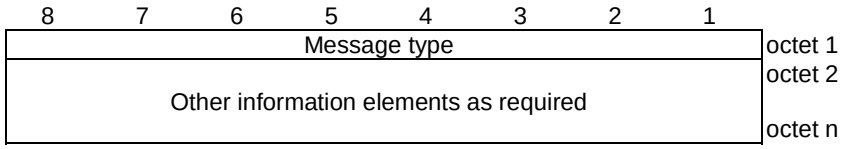

Figure 15.2.1-2: General message organization example

Unless specified otherwise in the message descriptions of subclause 15.1, a particular information element shall not be present more than once in a given message.

The sending entity shall set value of a spare bit to zero. The receiving entity shall ignore value of a spare bit

The sending entity shall not set a value of an information element to a reserved value. The receiving entity shall discard message containing an information element set to a reserved value.

15.2.2 Message type

The purpose of the Message type information element is to identify the type of the message.

The value part of the Message type information element is coded as shown in Table 15.2.2-1.

The Message type information element is a type 3 information element with a length of 1 octet.

Table 15.2.2-1: Message types

Bits 8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	GROUP CALL PROBE
0	0	0	0	0	0	1	0	GROUP CALL ANNOUNCEMENT
0	0	0	0	0	0	1	1	GROUP CALL ACCEPT
0	0	0	0	0	1	0	0	GROUP CALL EMERGENCY END
0	0	0	0	0	1	0	1	GROUP CALL IMMINENT PERIL END
0	0	0	0	0	1	1	0	GROUP CALL BROADCAST
0	0	0	0	0	1	1	1	GROUP CALL BROADCAST END
0	0	0	0	1	0	0	0	PRIVATE CALL SETUP REQUEST
0	0	0	0	1	0	0	1	PRIVATE CALL RINGING
0	0	0	0	1	0	1	0	PRIVATE CALL ACCEPT
0	0	0	0	1	0	1	1	PRIVATE CALL REJECT
0	0	0	0	1	1	0	0	PRIVATE CALL RELEASE
0	0	0	0	1	1	0	1	PRIVATE CALL RELEASE ACK
0	0	0	0	1	1	1	0	PRIVATE CALL ACCEPT ACK
0	0	0	0	1	1	1	1	PRIVATE EMERGENCY CALL CANCEL
0	0	0	1	0	0	0	0	PRIVATE EMERGENCY CALL CANCEL ACK
0	0	0	1	0	0	0	1	GROUP EMERGENCY ALERT
0	0	0	1	0	0	1	0	GROUP EMERGENCY ALERT ACK
0	0	0	1	0	0	1	1	GROUP EMERGENCY ALERT CANCEL
0	0	0	1	0	1	0	0	GROUP EMERGENCY ALERT CANCEL ACK
All other values are reserved.								

15.2.3 Call identifier

The purpose of the Call identifier information element is to uniquely identify the call.

The Call identifier information element is coded as shown in Figure 15.2.3-1 and Table 15.2.3-1.

The Call identifier information element is a type 3 information element with a length of 2 octets.

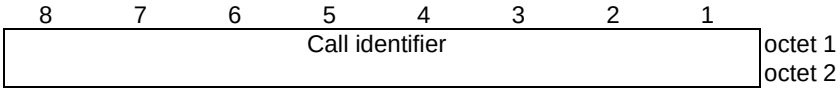

Figure 15.2.3-1: Call identifier information element

Table 15.2.3-1: Call identifier information element

Call identifier value (octet 1 to 2) The Call identifier contains a number uniquely identifying the call.

15.2.4 Refresh interval

The refresh interval information identifier is used to indicate the minimum time period between successive periodic messages;

The Refresh interval information element is coded as shown in Figure 15.2.4-1 and Table 15.2.4-1.

The Refresh interval information element is a type 3 information element with a length of 2 octets.

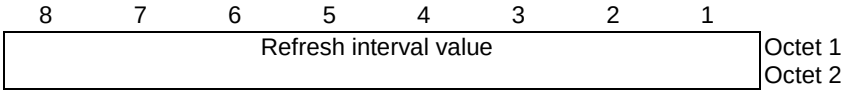

Figure 15.2.4-1: Refresh interval

Table 15.2.4-1: Refresh interval information element

Refresh interval value (octet 1 to 2) The Refresh interval contains a number denoting the minimum time interval (milliseconds) between two successive periodic announcements.

15.2.5 MCPTT group ID

The MCPTT group ID information element is used to indicate the destination MCPTT group identifier;

The MCPTT group ID information element is coded as shown in Figure 15.2.5-1 and Table 15.2.5-1.

The MCPTT group ID information element is a type 6 information element.

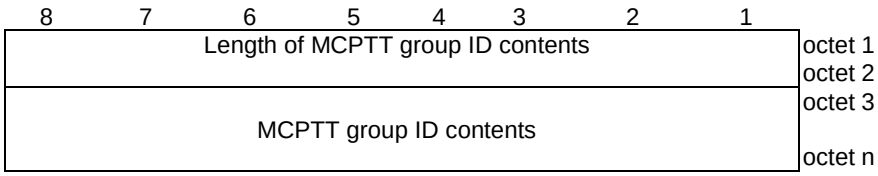

Figure 15.2.5-1: MCPTT group ID information element

Table 15.2.5-1: MCPTT group ID information element

MCPTT group ID is contained in octet 3 to octet n; Max value of 65535 octets.

15.2.6 SDP

The purpose of the SDP information element is to contain SDP message.

The SDP information element is coded as shown in Figure 15.2.6-1 and Table 15.2.6-1.

The SDP information element is a type 6 information element.

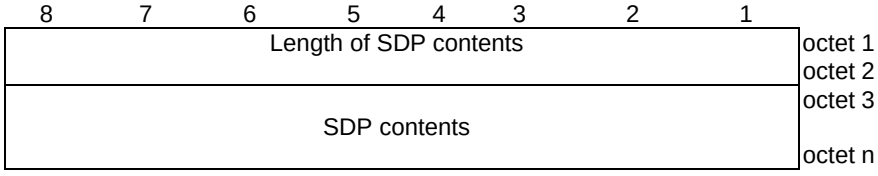

Figure 15.2.6-1: SDP information element

Table 15.2.6-1: SDP information element

SDP message container contents (octet 3 to octet n); Max value of 65535 octets. This information element contains SDP message as defined in Section 10.2.1.1.2 or 11.2.1.1.2.

15.2.7 Commencement mode

The purpose of the Commencement mode information element is to identify the type of the commencement mode of the private call.

The value part of the Commencement mode information element is coded as shown in Table 15.2.7-1.

The Commence mode information element is a type 3 information element with a length of 1 octet.

Table 15.2.7-1: Commencement mode

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	AUTOMATIC COMMENCEMENT MODE
0 0 0 0 0 0 0 1	MANUAL COMMENCEMENT MODE
All other values are reserved.	

15.2.8 Reason

The purpose of the Reason information element is to indicate the reason of the reject.

The Reason information element is coded as shown in table 15.2.8-1.

The Reason information element is a type 3 information element.

Table 15.2.8-1: Reason type

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	REJECT
0 0 0 0 0 0 0 1	MEDIA FAILURE
0 0 0 0 0 0 1 0	BUSY
0 0 0 0 0 0 1 1	E2E SECURITY CONTEXT FAILURE
0 0 0 0 0 1 0 0	FAILED
All other values are reserved.	

15.2.9 Confirm mode indication

The purpose of the Confirm mode indication information element is to indicate that the terminating MCPTT client is expected to confirm call acceptance.

The Confirm mode indication information element is coded as shown in figure 15.2.9-1.

The Confirm mode indication information element is a type 2 information element.

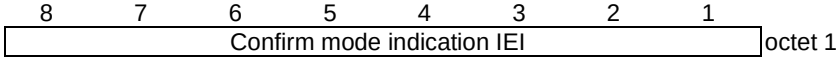

Figure 15.2.9-1: Confirm mode indication information element

15.2.10 MCPTT user ID

The MCPTT user ID information element is used to indicate an MCPTT user ID.

The MCPTT user ID information element is coded as shown in Figure 15.2.10-1 and Table 15.2.10-1.

The MCPTT user ID information element is a type 6 information element.

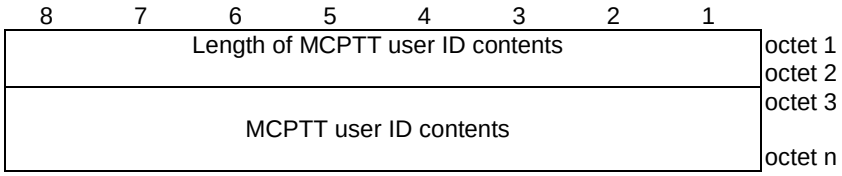

Figure 15.2.10-1: MCPTT user ID information element

Table 15.2.10-1: MCPTT user ID information element

MCPTT user ID is contained in octet 3 to octet n; Max value of 65535 octets.

15.2.11 Call type

The purpose of the Call type information element is to identify the type of the call.

The value part of the Call type information element is coded as shown in Table 15.2.11-1.

The Call type information element is a type 3 information element with a length of 1 octet.

Table 15.2.11-1: Call type

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 1	BASIC GROUP CALL
0 0 0 0 0 0 1 0	BROADCAST GROUP CALL
0 0 0 0 0 0 1 1	EMERGENCY GROUP CALL
0 0 0 0 0 1 0 0	IMMINENT PERIL GROUP CALL
0 0 0 0 0 1 0 1	PRIVATE CALL
0 0 0 0 0 1 1 0	EMERGENCY PRIVATE CALL
All other values are reserved.	

15.2.12 User location

The User location information element is used to indicate the current location of the MCPTT client;

The User location information element is coded as shown in Figure 15.2.12-1 and Table 15.2.12-1.

The User location information element is a type 6 information element.

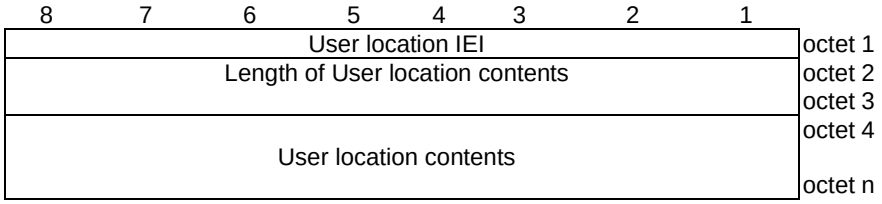

Figure 15.2.12-1: User location information element

Table 15.2.12-1: User location information element

User location is contained in octet 4 to octet n; Max value of 65535 octets.

The User location information element contains the LocationInfo structure defined in subclause 7.4 of 3GPP TS 29.199-9 [59].

15.2.13 Organization name

The Organization name information element is used to indicate the name of the organization to which the user belongs.

The Organization name information element is coded as shown in Figure 15.2.13-1 and Table 15.2.13-1.

The Organization name information element is a type 6 information element.

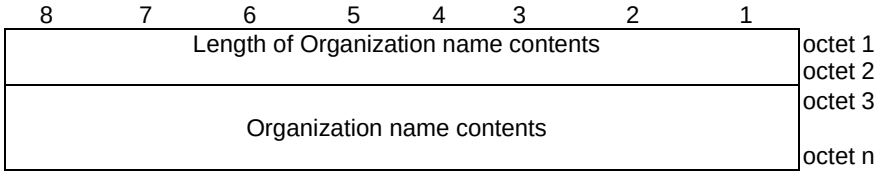

Figure 15.2.13-1: Organization name information element

Table 15.2.13-1: Organization name information element

Organization name is contained in octet 3 to octet n; Max value of 65535 octets.

15.2.14 Call start time

The Call start time information element is used to indicate the UTC time when a call was started.

The Call start time information element is coded as shown in Figure 15.2.14-1 and Table 15.2.14-1.

The Call start time information element is a type 3 information element with a length of 5 octets.

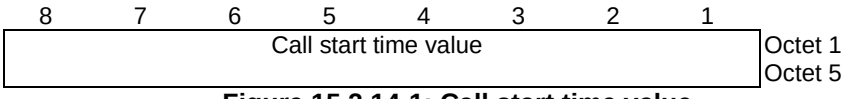

Figure 15.2.14-1: Call start time value

Table 15.2.14-1: Call start time value

Call start time value (octet 1 to 5) The Call start time value is an unsigned integer containing UTC time of the time when a call was started, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).

15.2.15 Last call type change time

The Last call type change time information identifier is used to indicate the last UTC time when a call priority was changed.

The Last call type change time information element is coded as shown in Figure 15.2.15-1 and Table 15.2.15-1.

The Last call type change time information element is a type 3 information element with a length of 5 octets.

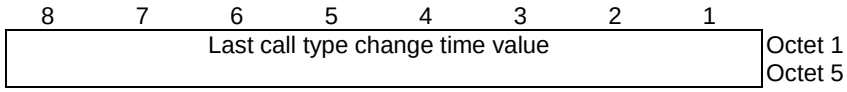

Figure 15.2.15-1: Last call type change time value

Table 15.2.15-1: Last call type change time value

Last call type change time (octet 1 to 5) The Last call type change time value is an unsigned integer containing UTC time of the time when a call priority was changed, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).

15.2.16 Probe response

The purpose of the probe response information element is to indicate that the GROUP CALL ANNOUNCEMENT message was sent in response of a GROUP CALL PROBE message.

The probe response information element is coded as shown in figure 15.2.16-1.

The probe response is a type 2 information element.

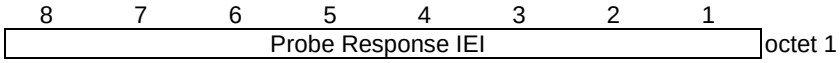

Figure 15.2.16-1: Probe response information element

Annex A (informative): Signalling flows

A.0 General

The flows in this Annex are only for the purposes of illustration and are not guaranteed to be up-to-date.

A.1 Group regrouping flow

A.1.1 General

This clause describes how a temporary group call as the result of a group regroup operation is established.

A.1.2 Use case description

The police and a private security company cooperate during a fair. A temporary prearranged group is created as specified in TS 24.481 [31] to allow the policemen and security personal to communicate.

The temporary group consists of two groups of policemen and a group of security personal from the private security company. One of the groups of policemen is called in from another town. A dispatcher from the police creates the temporary group. The dispatcher is added to the group of policemen hosted by the controlling MCPTT function A.

Table A.1.2-1 shows the group coding details.

Table A.1.2-1: Group coding details

MCPTT group identity	Hosted by	Group type	MCPTT group members
mcptt-group-A-B@mcptt-op.gov	controlling MCPTT function A	Temporary group	mcptt-group-A1@mcptt-op.gov
			mcptt-group-B@mcptt-city1.net
			mcptt-group-A2@mcptt-op.gov
mcptt-group-A1@mcptt-op.gov	controlling MCPTT function A	Prearranged group	mcptt-id-A2@mcptt-op.gov
mcptt-group-B@mcptt-city1.net	non-controlling MCPTT function B	Prearranged group	mcptt-id-B@mcptt-city1.net
mcptt-group-A2@mcptt-op.gov	non-controlling MCPTT function A	Prearranged group	mcptt-id-A3@mcptt-op.gov

For readability reasons all prearranged groups have only one member. Table A.1.2-1 shows the group member coding details.

Table A.1.2-2: Group member coding details

MCPTT ID of group member	Registered public user identity	MCPTT client name	IP address audio / floor control port number (NOTE 2)
mcptt-id-A1@mcptt-op.gov	sip:userA1@ims-op.net	MCPTT client A1	5555::aaa:bbb:ccc:eee 3456 / 3457
mcptt-id-A2@mcptt-op.gov	sip:userA2@ims-op.net	MCPTT client A2	5555::aaa:ccc:aaa:bbb 26456 / 26457 (NOTE 1)
mcptt-id-A3@mcptt-op.gov	sip:userA3@ims-op.net	MCPTT client A3	5555::bbb:aaa:ccc:aaa 25644 / 25645
mcptt-id-B@mcptt-city1.net	sip:userB@ims-op.net	MCPTT client B	5555::baa:abb:ddd:ccc 62122 / 62122

NOTE 1: A pre-established session is used and the IP address and port numbers of the participating MCPTT function A2 is used.
NOTE 2: The IP address is the same as for the registered contact.

Each MCPTT user is served by a different MCPTT function. Table A.1.2-3 shows the Participating MCPTT functions coding details.

Table A.1.2-3: Participating MCPTT functions coding details

Functional entity	Public service identity	IP address audio / floor control port number
participating MCPTT function A1	sip:pf-A1.ims-op.net	5555::aaa:bbb:ccc:eef 7890 / 7891
participating MCPTT function A2	sip:pf-A2.ims-op.net	5555::aaa:ccc:aaa:bbb 26456 / 26457
participating MCPTT function A3	sip:pf-A3.ims-op.net	5555::aaa:ccc:aaa:ccc 18412 / 18413
participating MCPTT function B	sip:pf-B.ims-op.net	5555::aaa:bbb:ccc:eef 16412 / 16413

Each group is hosted by a different MCPTT server. Table A.1.2-4 shows the Controlling and non-controlling MCPTT functions coding details.

Table A.1.2-4: Controlling and non-controlling MCPTT functions coding details

Functional entity	Public service identity	MCPTT session identifier	IP address audio / floor control port number
controlling MCPTT function A	sip:cf-A.ims-op.net	session@cf-A@ims-op.net	5555::aaa:bbb:ddd:aaa 23124 / 23125
non-controlling MCPTT function A	sip:cf-A2.ims-op.net	sessionA@cf-A2@ims-op.net	5555::aaa:bbb:ddd:eee 12344 / 12345
non-controlling MCPTT function B	sip:cf-B.ims-op.net	sessionB@cf-B@ims-op.net	5555::aaa:bbb:ddd:ddd 34456 / 34457

A.1.3 Signalling flow

The temporary group consists of a group A1 (police), group A2 (police in other town) and a group B (security company in a partner system).

For the mcptt-id-B@mcptt-city1.net the controlling MCPTT function is using the connection model in figure 5.3.2-5.

For the mcptt-id-A3@mcptt-op.gov the controlling MCPTT function is using the connection model in figure 5.3.2-2.

Preconditions:

1) the temporary group mcptt-group-A-B is already created and all members are affiliated to the group;

2) this is not an emergency or imminent peril call;

3) MCPTT client A2 has a pre-established session and the MCPTT services setting for the commencement mode is auto-answer;

4) MCPTT client A3 has no pre-established session and the MCPTT services setting for the commencement mode is manual-answer;

5) MCPTT client has no pre-established session and the MCPTT services setting for queueing the commencement mode is auto-answer;

6) the IMS service provider (ims-op.net) is the same for all groups;

7) the flow does not consider confidentiality and integrity protection; and

8) non-controlling model used between the Primary and the partner is the "untrusted" model.

Figure A.1.3-1 shows the signalling flow when the controlling MCPTT function invites the prearranged groups consisting in the temporary group.

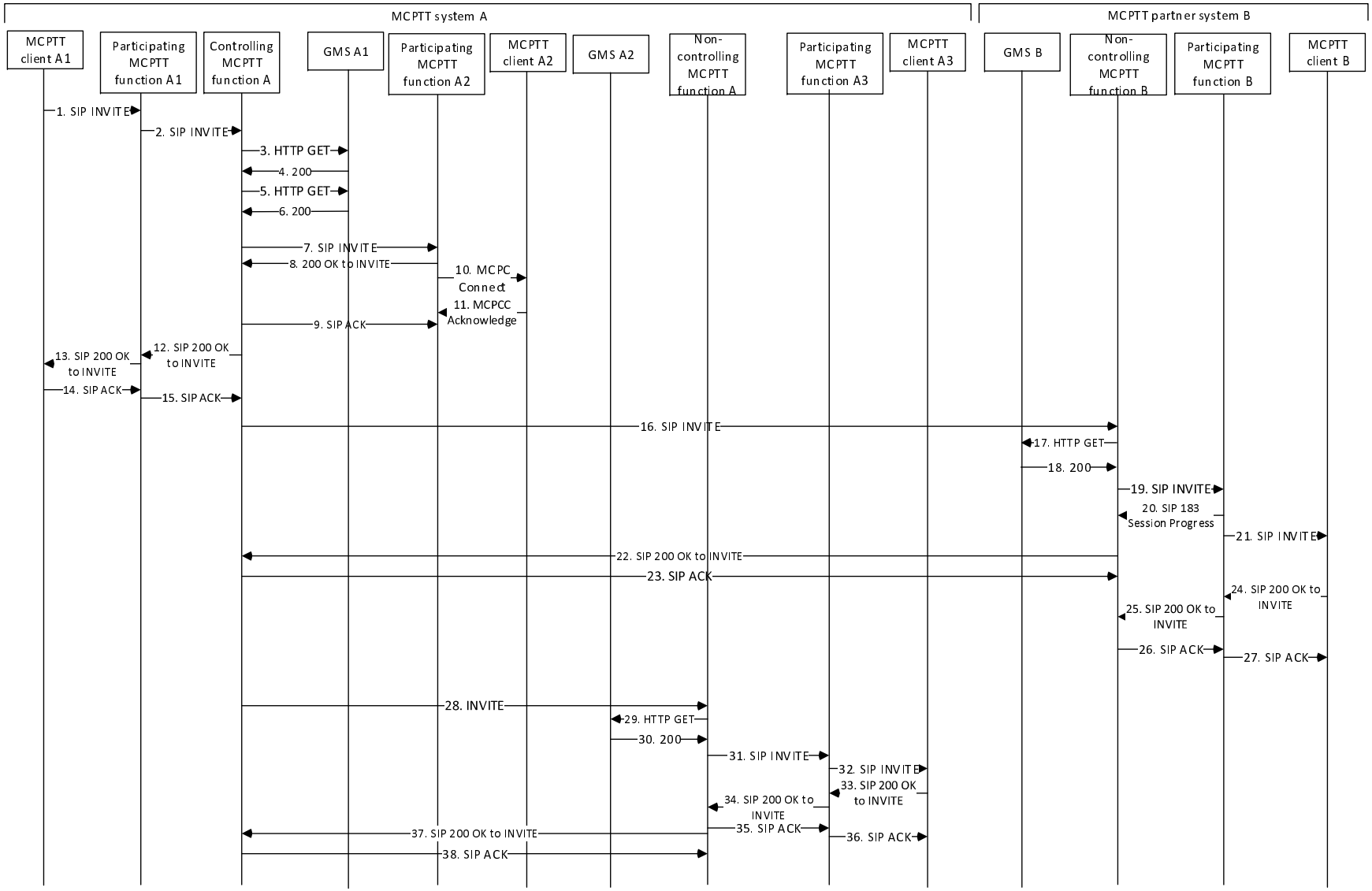

Figure A.1.3-1: Temporary prearranged group call setup

The steps of the flow are as follows:

NOTE 1: The parameters in the coding parts are only those specified in the normative part of the present document. For information about other parameters, see 3GPP TS 24.229 [4].

1) SIP INVITE request (MCPTT client A1 to participating MCPTT function A1) - see example in table A.1.3-1

Upon receiving a request from an MCPTT user A1 to establish an MCPTT temporary group session the MCPTT client A1 sends a SIP INVITE request towards the participating MCPTT function A1 according to 3GPP TS 24.229 [4].

Table A.1.3-1: SIP INVITE request (MCPTT client A1 to participating MCPTT function A1)

```
INVITE sip: pf-A1.ims-op.net SIP/2.0
Accept-Contact: *;+g.3gpp.mcptt;require;explicit,+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt;require;explicit
P-Preferred-Service:urn:urn-7:3gpp-service.ims.icsi.mcptt
Supported: timer
Session-Expires: 3600;refresher=uac
Contact: <sip:[5555::aaa:bbb:ccc:eee]>;g.3gpp.mcptt;g.3gpp.icsi-ref=urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt
P-Preferred-Identity:<sip:userA1@ims-op.net>

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ccc:eee
m=audio 3456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=maxptime:20
i=speech
m=application 3457 udp mcptt
a=fmtp:MCPTT mc_queueing;mc_implicit_request
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-group-T@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1–
```

Request-URI: Contains the public service identity of the participating MCPTT function serving the MCPTT user.

Accept-Contact: Contains the g.3gpp.mcptt feature tag.

P-Preferred-Service: Contains the ICSI for MCPTT.

Contact: Contains the registered contact and the g.3gpp.mcptt feature tag.

P-preferred-Identity: Contains the public user identity of the MCPTT user.

mcptt-info: The application/vnd.3gpp.mcptt-info+xml contains the <mcptt-Params> element with the <session-type> element set to "prearranged" and the <mcptt-request-uri> element set to "mcptt-group-T@mcptt-op.gov".

SDP offer: Contains a media-level section for the MCPTT speech media stream and a media-level section for the media-floor control entity indicating that of floor requests is supported ("mc:queueing") and that the SIP INVITE request is an implicit floor request ("mc_implicit_request").

2) SIP INVITE request (participating MCPTT function A1 to controlling MCPTT function A) - see example in table A.1.3-2

Upon receiving 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 authorizes the MCPTT user to initiate the prearranged group call and since the MCPTT user is authorized, the participating MCPTT function A1 forwards the SIP INVITE request according to 3GPP TS 24.229 [4].

Table A.1.3-2: SIP INVITE request (participating MCPTT function A to controlling MCPTT function A)

```
INVITE sip: cf-A.ims-op.net SIP/2.0
Accept-Contact:
P-Asserted-Service:
Supported:
Session-Expires:
Contact:
P-Asserted-Identity:<sip:userA1@ims-op.net>

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ccc:eef
m=audio 7890 RTP/AVP 97
a=
a=
i=
m=application 7891 udp mcptt
a=
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-group-T@mcptt-city1.gov</>
    <mcptt-calling-user-id>mcptt-id-A1@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1--
```

Request-URI: Updated to include the public service identifier of the MCPTT server owning the mcptt-group-T@mcptt-city1.gov.

mcptt-info: The application/vnd.3gpp.mcptt-info+xml is updated to include the MCPTT ID of the MCPTT user in the <mcptt-calling-user-id> element. The participating MCPTT function A1 determines the MCPTT-ID using the public user identity to locate the binding formed during service authorisation.

SDP offer: The SDP offer is updated to include the IP address and port numbers of the participating MCPTT function.

3) HTTP GET request (controlling MCPTT function A to GMS A)

Upon receipt of the "SIP INVITE request for controlling MCPTT function of an MCPTT group" the controlling MCPTT functions fetches the group document mcptt-group-T@mcptt-op.gov from the GMS A.

4) HTTP 200 response (GMS A to controlling MCPTT function A)

The GMS A returns the mcptt-group-T@mcptt-op.gov group document and the document indicates that this is a temporary group consisting of mcptt-group-A1@mcptt-op.gov, mcptt-group-B@mcptt-city1.net and mcptt-group-A2@mcptt-op.gov.

5) HTTP GET request (controlling MCPTT function A to GMS A)

Since the mcptt-id-A1@mcptt-op.gov is affiliated to the mcptt-group-A1@mcptt-op.gov the controlling MCPTT function fetches the group document from GMS A by means of a HTPP GET request as described in 3GPP TS 24.481 [31].

6) HTTP 200 response (GMS A to controlling MCPTT function B)

The GMS A returns the mcptt-group-A1@mcptt-op.gov group document with the list of group members in a HTTP 200 response as described in 3GPP TS 24.481 [31].

The controlling MCPTT function verifies that the mcptt-id-A1@mcptt-op.gov is authorized to initiate a prearranged group call.

The following steps describe the invitation of the group member mcptt-id-A@mcptt-op.gov using a pre-established session between the participating MCPTT function A2 and MCPTT client A2. Other members can be invited using the same method or using on-demand session signalling.

7) SIP INVITE request (controlling MCPTT function A to participating MCPTT function A2) - see example in table A.1.3-7

The controlling MCPTT function sends an initial SIP INVITE request towards the participating MCPTT function A2 according to 3GPP TS 24.229 [4].

Table A.1.3-7: SIP INVITE request (controlling MCPTT function A to participating MCPTT function A2)

```
INVITE sip: pf-A2.ims-op.net SIP/2.0
Accept-Contact: *;+g.3gpp.mcptt;require;explicit,+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt;require;explicit
P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mcptt
Supported:timer
Session-Expires:3600
Contact: <sip:session@cf-A@ims-op.net:66350>;g.3gpp.mcptt;isfocus;g.3gpp.icsi-ref=urn%3Aurn-
7%3A3gpp-service.ims.icsi.mcptt
P-Asserted-Identity:<sip:cf-a@ims-op.net>

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ddd:aaa
m=audio 23124 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=maxptime:20
i=speech
m=application 23125 udp mcptt
a=fmtp:MCPTT mc_queueing;
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-id-A2@mcptt-op.gov</>
    <mcptt-calling-group-id>mcptt-group-T@mcptt-op.gov</>
    <mcptt-calling-user-id>userA1@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1--
```

Request-URI: Contains the public service identity of the participating MCPTT function A2 associated to the MCPTT user mcptt-id-A2@mcptt-op.gov.

Contact: Contains the MCPTT session identity.

P-Asserted-Identity: Contains the public service identity of the controlling MCPTT function A.

mcptt-info Is copied from the received INVITE request and updated to include the "mcptt-id-A2@mcptt-op.gov" in the <mcptt-request-uri> element and mcptt-group-T@mcptt-op.gov in the <mcptt-calling-group-id> element.

SDP offer: The SDP offer is based on the received SDP offer where the IP address and port numbers are replaced with the IP address and port numbers of the controlling MCPTT function. The media-level section for the media-floor control entity is indicating that queueing of floor requests is supported ("mc:queueing").

8) SIP 200 (OK) response (participating MCPTT function A2 to controlling MCPTT function A) - see example in table A.1.3-8

The participating MCPTT function detects that there is a pre-established session to the MCPTT client A2 where negotiated MCPTT speech media stream parameters and media-floor control entity 'fmtp' attributes matches the incoming SIP INVITE request and that the MCPTT service setting for commencement mode is set to "auto-answer".

The participating MCPTT function A2 sends a SIP 200 (OK) response to the controlling MCPTT function A according to 3GPP TS 24.229 [4].

Table A.1.3-8: SIP 200 (OK) response (participating MCPTT function A2 to controlling MCPTT function A)

```
SIP/2.0 200 OK
Session-Expires:3600;refresher=uac
Require: timer
P-Asserted-Identity:<sip:userA2@ims-op.net>
Contact: <sip:[5555::aaa:ccc:aaa:bbbb]>; g.3gpp.mcptt;
Supported: tdialog, norefersub, explicitsub, nosub
P-Answer-State:Unconfirmed

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:ccc:aaa:bbbb
m=audio 26456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=maxptime:20
i=speech
m=application 26457 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-called-party-id>mcptt-id-A2@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1–
```

P-Asserted-Identity: Contains a public user identity of the sip: userA2@ims-op.net.

Contact: Contains a URI that identifies the session in the participating MCPTT function A2.

P-Answer-State: Contains the value "Unconfirmed" to indicate that the participating MCPTT function A2 sent this on behalf of the MCPTT A2.

SDP answer: The SDP answer is based on the received SDP offer and is updated to IP address and port numbers of the participating MCPTT function A2. The media-floor control entity 'fmtp' attributes includes the "mc_queueing" to indicate that queueing is supported.

9) SIP ACK request (controlling MCPTT function A to participating MCPTT function A2)

The controlling MCPTT function A acknowledge the SIP 200 (OK) response by means of the SIP ACK request.

10) MCPC Connect message (participating MCPTT function to MCPTT client B)

Since the MCPTT client B has a pre-established session the participating MCPTT function B uses the pre-established session to invite the MCPTT client B by means of a MCPC Connect messages as described in 3GPP TS 24.380 [5] annex A.

11) MCPC Acknowledgement message (MCPTT client B to participating MCPTT B)

The MCPTT client B acceptes the invitation and sends an MCCP Acknowledge message as as described in 3GPP TS 24.380 [5] annex A.

12) SIP 200 (OK) response (controlling MCPTT function A to participating MCPTT function A1) - see example in table A.1.3-12

Upon receiving the SIP 200 (OK) response from the participating MCPTT function A2, the controlling MCPTT function A interacts with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.3 and sends the SIP 200 (OK) towards the participating MCPTT function A1 according to 3GPP TS 24.229 [4].

NOTE 2: When more than one MCPTT user is invited (not done in this example) then when receiving additional SIP 200 (OK) responses from other participating MCPTT functions, the controlling MCPTT function sends the SIP ACK request towards the other participating MCPTT functions and interacts with the media plane as specified in subclause 6.3 i.e. there is no SIP signalling sent towards the MCPTT client A1.

NOTE 3: If there more than one user in the group, the 200 (OK) response is not sent if the acknowledged timeout value for the group is running if some members of the group are marked as <on-network-required> as specified in 3GPP TS 24.481 [31], and responses are not received from those members.

Table A.1.3-12: SIP 200 (OK) response (controlling MCPTT function A to participating MCPTT function A1)

```
SIP/2.0 200 OK
Session-Expires:3600;refresher=uac
Require: timer
P-Asserted-Identity:<sip:cf-A.ims-op.net>
Contact: <sip:[5555::aaa:bbb:ddd:bbbb]>; +g.3gpp.mcptt;+g.3gpp.icsi-ref; isfocus
Supported: tdialog, norefersub, explicitsub, nosub
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ddd:bbbb
m=audio 23124 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=maxptime:20
i=speech
m=application 23125 udp mcptt
a=fmtp:MCPTT mc_queueing;mc_implicit_request
```

P-Asserted-Identity: Contains the public user identifier identifying the controlling MCPTT function.

Contact: Contains the MCPTT session identifier and the g.3gpp.icsi-ref and isfocus media feature tags.

SDP answer: Contains the SDP answer to the SDP offer received from the participating MCPTT function A2 updated with the IP address and port numbers of the controlling MCPTT function. The media-level section for the media-floor control entity acknowledges that queueing is supported ("mc_queueing") and that the SIP INVITE request is accepted as an implicit floor request.

13) SIP 200 (OK) response (participating MCPTT function A to MCPTT client A) - see example in table A.1.3-13

The participating MCPTT function A1 interacts with the media plane as specified in 3GPP TS 24.380 [5] subclause 6.4 and sends the SIP 200 (OK) response towards the MCPTT client A1.

Table A.1.3-13: SIP 200 (OK) response (participating MCPTT function A to MCPTT client A1)

```
SIP/2.0 200 OK
Session-Expires:
Require:
P-Asserted-Identity:
Contact:
Resouce-Share: media-sharing; session-initiator; rules="k1::UL"; timestamp=55688
Priority-Share:allowed
Supported: tdialog
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:ccc:aaa:bbb
m=audio 7890 RTP/AVP 97
a=
a=
a=
m=application 7891 udp mcptt
a=
```

Resource-Share: Contains a new sharing key along with indication that MCPTT speech media can be shared in the uplink (UL) direction. The value "k1" is the key that P-CSCF can use to identify media streams towards MCPTT client A1 that can share media.

Priority-Share: The Priority-Share header field is set to "allowed" indicating that priority sharing can be applied by IMS.

SDP answer: Contains the SDP answer received from the controlling MCPTT function updated with the IP address and port numbers of the participating MCPTT function.

14)-15) SIP ACK request (MCPTT client A1 to controlling MCPTT function A via participating MCPTT function A1)

The MCPTT client A1 acknowledges the receipt of the SIP 200 (OK) response by means of a SIP ACK request. The ACK request is forwarded by the participating MCPTT function A1 to the controlling MCPTT function A.

16) SIP INVITE request (controlling MCPTT function A to non-Controlling MCPTT function C) - see example in table A.1.3-16

Since the GMS storing the group document of the "mcptt-group-B@mcptt-city1.net" is not available to the controlling MCPTT function A, the controlling MCPTT function A decides to use the non-controlling MCPTT function connectivity model (see figure 5.3.2-5) and sends a SIP INVITE request towards the MCPTT server hosting "mcptt-group-B@mcptt-city1.net" according to 3GPP TS 24.229 [4].

Table A.1.3-16: SIP INVITE request (controlling MCPTT function A to non-Controlling MCPTT function B)

```
INVITE sip:cf-B.ims-op.net SIP/2.0
Accept-Contact: *;+g.3gpp.mcptt;require;explicit,+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt;require;explicit
P-Asserted-Service:urn:urn-7:3gpp-service.ims.icsi.mcptt
Supported:timer
Session-Expires:3600
Contact: <sip:session@cf-A@ims-op.net:66350>;g.3gpp.mcptt;isfocus;g.3gpp.icsi-ref=urn%3Aurn-
7%3A3gpp-service.ims.icsi.mcptt
P-Asserted-Identity:<sip:cf-a@ims-op.net>

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ddd:aaa
m=audio 23124 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=maxptime:20
i=speech
m=application 23125 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-group-B@mcptt-city1.net</>
    <mcptt-calling-user-id>userA1@mcptt-op.gov</>
    <mcptt-calling-group-id>mcptt-group-T@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1--
```

Request-URI: Contains the public service identity of the MCPTT server hosting the "mcptt-group-B@mcptt-city1.net".

Contact: Contains the MCPTT session identity.

mcptt-info: Is copied from the received INVITE request and updated to include the "mcptt-group-B@mcptt-city1.net" in the <mcptt-request-uri> element and mcptt-group-T@mcptt-op.gov in the <mcptt-calling-group-id> element.

SDP offer: Is based on the received SDP offer where the IP address and port numbers are replaced with the IP address and port numbers of the controlling MCPTT function. The media-level section for the media-floor control entity is indicating that queueing is supported ("mc:queueing").

17) HTTP GET request (controlling MCPTT function A to GMS B)

Since mcptt-group-B@mcptt-city1.net is hosted by the non-controlling MCPTT function B the group document is fetched from GMS B.

The group document are fetched by means of a HTPP GET request as described in 3GPP TS 24.481 [31].

18) HTTP 200 response (GMS B to controlling MCPTT function B)

The GMS B returns the mcptt-group-B@mcptt-city1.net group document with the list of group members in a HTTP 200 response as described in 3GPP TS 24.481 [31].

The following steps describes the invitation of one group member, mcptt-id-B@mcptt-city1.net, using an on-demand session between the participating MCPTT function B and MCPTT client B. Other members can be invited using the same method or using pre-established session.

19) SIP INVITE request (non-controlling MCPTT function B to participating MCPTT function B) - see example in table A.1.3-19

The non-controlling MCPTT function B invites the MCPTT user "mcptt-id-B@mcptt-city1.net" to the session by sending and SIP INVITE request towards the terminating network in accordance with 3GPP TS 24.229 [4].

Table A.1.3-19: SIP INVITE request (non-Controlling MCPTT function B to participating MCPTT function B)

```
INVITE sip: pf-B.ims-op.net SIP/2.0
Accept-Contact:
P-Asserted-Service:
Supported:
Session-Expires:
Contact: <sip:sessionB@cf-B@ims-op.net:45678>;g.3gpp.mcptt; isfocus; g.3gpp.icsi-ref=urn%3Aurn-
7%3A3gpp-service.ims.icsi.mcptt
P-Asserted-Identity:<sip:cf-b@ims-op.net>

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ddd:ddd
m=audio 34456 RTP/AVP 97
a=
a=
a=
i=
m=application 34457 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-id-B@mcptt-city1.net</>
    <mcptt-calling-user-id>mcptt-id-A@mcptt-op.gov</>
    <mcptt-calling-group-id>mcptt-group-T@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1--
```

Contact: Contains a new MCPTT session identity and can be used by the members to rejoin the session.

NOTE 4: The MCPTT session identity received from the controlling MCPTT function A cannot be used since when a member of group mcptt-group-B@mcptt-city1.net rejoins the session, the member shall rejoin the session in the non-controlling MCPTT function B and not the session in the controlling MCPTT function A.

P-Asserted-Identity: Contains the public service identity of the non-controlling MCPTT function B.

mcptt-info: The identity of the invited MCPTT user mcptt-id-B@mcptt-city1.net is added.

SDP offer: The SDP offer is a copy of the received SDP offer updated with the IP address and port numbers of the non-controlling MCPTT function B.

20) SIP 183 (Session Progress) response (participating MCPTT function B to non-Controlling MCPTT function B) - see example in table A.1.3-20

The participating MCPTT function B sends a SIP 183 (Session Progress) response towards the non-controlling MCPTT function B according to 3GPP TS 24.229 [4].

Table A.1.3-20: SIP 183 (Session Progress) response (participating MCPTT function B non-Controlling MCPTT function B)

```
SIP/2.0 183 Session Progress
P-Asserted-Identity:
Contact: <sip:[5555::aaa:bbb:ccc:eef]>;+g.3gpp.mcptt;,+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt
P-Answer-State:Unconfirmed
```

P-Answer-State: Contains the "Unconfirmed" indication acknowledging the automatic commencement mode.

21) SIP INVITE request (participating MCPTT function B to MCPTT client B) - see example in table A.1.3-21

The participating MCPTT function B sends the SIP INVITE request towards the MCPTT client B according to 3GPP TS 24.229 [4].

Table A.1.3-21: SIP INVITE request (participating MCPTT function B to MCPTT client B)

```
INVITE sip: userB@ims-op.net SIP/2.0
Accept-Contact:
P-Asserted-Service:
Supported:timer;tdialog
Session-Expires:refresher;uac
Contact:
Resouce-Share: media-sharing; session-receiver; rules="k2::UL"; timestamp=55750
Priority-Share:allowed
P-Asserted-Identity:<sip:cf-b@ims-op.net>
Answer-Mode:Auto

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ccc:eef
m=audio 16412 RTP/AVP 97
a=
a=
a=
i=
m=application 16413 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-id-B@mcptt-city1.net</>
    <mcptt-calling-user-id>userA1@mcptt-op.gov</>
    <mcptt-calling-group-id>mcptt-group-T@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1--
```

Request-URI: Contains the public user identity of the mcptt-id-B@mcptt-city1.net.

Resource-Share: Contains a new sharing key along with indication that MCPTT speech media can be shared in the uplink (UL) direction. The value "k2" is the key that P-CSCF can use to identify media streams towards MCPTT client A2 that can share media.

Priority-Share: The Priority-Share header field is set to "allowed" indicating that priority sharing can be applied by IMS.

Answer-Mode: The MCPTT service setting is "auto-answer" so the participating MCPTT function includes the value "auto" in the Answer-Mode header field.

SDP offer: The SDP offer is a copy of the received SDP offer updated with the IP address and port numbers of the participating MCPTT function B.

22) SIP 200 (OK) response (non-controlling MCPTT function B to controlling MCPTT function A) - see example in table A.1.3-22

Upon receipt of the first SIP 200 (OK) response from the participating MCPTT function B serving the invited MCPTT user B in the prearranged group mcptt-group-C@mcptt-city1.net, the non-controlling MCPTT function interact with the media plane as specified in 3GPP TS 24.380 [5] and sends the SIP 200 (OK) response towards the controlling MCPTT function A in accordance with 3GPP TS 24.229 [4].

NOTE 6: The non-controlling function translates the SIP 183 (Session Progress) response with a P-Answer-State header field set to "Auto" to a SIP 200 (OK) response only if the non-controlling function supports media-buffering otherwise a SIP 183 (Session Progress) response is sent.

Table A.1.3-22: SIP 200 (OK) response (non-controlling MCPTT function B to controlling MCPTT function A)

```
SIP/2.0 200 OK
Session-Expires:3600;refresher=uac
Require: timer
P-Asserted-Identity:<sip:cf-B.op.net>
Contact: <sip:[5555::aaa:bbb:ddd:ddd]>; g.3gpp.mcptt;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt
Supported: tdialog, norefersub, explicitsub, nosub
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ddd:ddd
m=audio 34456 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=maxptime:20
i=speech
m=application 34457 udp mcptt
a=fmtp:MCPTT mc_queueing
```

P-Asserted-Identity Contains a public service identity identifying the non-controlling MCPTT function B.

Contact Contains a contact address and the media feature tags g.3gpp.mcptt and g.3gpp.icsi-ref.

SDP Contains the SDP answer to the SDP offer received from the controlling MCPTT function A. The media-level section for the media-floor control entity acknowledges that queueing is supported ("mc_queueing").

NOTE 5: The SDP answer is based on the capabilities of the non-controlling MCPTT function and not based on the SIP 200 (OK) response received from the participating MCPTT function.

23) SIP ACK request (controlling MCPTT function A to MCPTT client B via non-controlling MCPTT function B and participating MCPTT function B)

The controlling MCPTT function acknowledges the receipt of the SIP 200 (OK) response by means of a SIP ACK request.

24)-25) SIP 200 (OK) response (MCPTT client B to non-controlling MCPTT function B via participating MCPTT function B) - see example in table A.1.3-24

Upon receiving the SIP INVITE request the MCPTT client B accepts the invitation, interacts with the media plane as specified in 3GPP TS 24.380 subclause 6.2 and sends the SIP 200 (OK) response towards the MCPTT server according to rules and procedures of 3GPP TS 24.229 [4].

Table A.1.3-24: SIP 200 (OK) response (MCPTT client B to non-controlling MCPTT function B via participating MCPTT function B)

```
SIP/2.0 200 OK
Session-Expires:3600;refresher=uas
Require: timer
Contact:<sip:[5555::baa:abb:ddd:cccc]>;+g.3gpp.mcptt;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt"
P-Asserted-Identity:<sip:userB@ims-op.net>
Supported: tdialog, norefersub, explicitsub, nosub
P-Answer-State:Confirmed
Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::baa:abb:ddd:cccc
m=audio 62122 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=maxptime:20
i=speech
m=application 62123 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-called-party-id>mcptt-id-B@mcptt-city1.net</>
  </mcptt-Params>
</mcpttinfo>
--boundary1–
```

Contact: Contains the registered contact and the g.3gpp.mcptt feature tag.

P-Answer-State: Contains the value "Confirmed" to indicate that the MCPTT client B sent the response.

SDP answer: The received SDP offer is accepted and updated with the IP address and port numbers of the MCPTT client B. The MCPTT client B confirms that queueing of floor requests are supported in the 'fmtp' attribute "mc_queueing".

The participating MCPTT function B updates the IP address and port numbers with the IP address and port numbers of the participating MCPTT function B.

26)-27) SIP ACK request (non-controlling MCPTT function B to MCPTT client B via participating MCPTT function B)

The non-controlling MCPTT function acknowledges the receipt of the SIP 200 (OK) response by means of a SIP ACK request.

28) SIP INVITE request (controlling MCPTT function A to non-controlling MCPTT function A) – see example in table A.1.3-28

Since the GMS storing the group document of the "mcptt-group-A2@mcptt-op.gov" is not available to the controlling MCPTT function A, the controlling MCPTT function A decides to use the non-controlling MCPTT function connectivity model (see figure 5.3.2-2) and sends a SIP INVITE request towards the MCPTT server hosting "mcptt-group-A2@mcptt-op.gov" in accordance with 3GPP TS 24.229 [4].

Table A.1.3-28: SIP INVITE request (controlling MCPTT function A to non-Controlling MCPTT function A)

```
INVITE sip: cf-A2.ims-op.net SIP/2.0
Accept-Contact: *;+g.3gpp.mcptt;require;explicit,+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt;require;explicit
P-Asserted-Service:urn:urn-7:3gpp-service.ims.icsi.mcptt
Supported:timer
Session-Expires:3600
Contact: <sip:session@cf-A@ims-op.net:66350>;g.3gpp.mcptt;isfocus;g.3gpp.icsi-ref=urn%3Aurn-
7%3A3gpp-service.ims.icsi.mcptt
P-Asserted-Identity:<sipcf-a@ims-op.net>

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ddd:aaa
m=audio 23124 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=maxptime:20
i=speech
m=application 23125 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-group-A2@mcptt-op.gov</>
    <mcptt-calling-user-id>userA1@mcptt-op.gov</>
    <mcptt-calling-group-id>mcptt-group-T@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>

--boundary1--
```

Request-URI: Contains the public service identity of the MCPTT server hosting the "mcptt-group-A2@mcptt-op.gov".

Contact: Contains the MCPTT session identity.

mcptt-info: Is copied from the received INVITE request and updated to include the "mcptt-group-A2@mcptt-op.gov" in the <mcptt-request-uri> element and mcptt-group-T@mcptt-op.gov in the <mcptt-calling-group-id> element.

SDP offer: Is based on the received SDP offer where the IP address and port numbers are replaced with the IP address and port numbers of the controlling MCPTT function. The media-level section for the media-floor control entity is indicating that queueing is supported ("mc:queueing").

29) HTTP GET request (controlling MCPTT function A to GMS B)

Since mcptt-group-A@mcptt-city1.net is hosted by the non-controlling MCPTT function A the group document is fetched from GMS A2.

The group document is fetched by means of a HTPP GET request as described in 3GPP TS 24.481 [31].

30) HTTP 200 response (GMS B to controlling MCPTT function B)

The GMS B returns the mcptt-group-A2@mcptt-op.gov group document with the list of group members in a HTTP 200 response as described in 3GPP TS 24.481 [31].

The following steps describes the invitation of one group member, mcptt-id-A@mcptt-op.gov, using an on-demand session between the participating MCPTT function B and MCPTT client B. Other members can be invited using the same method or using pre-established session.

31) SIP INVITE request (non-controlling MCPTT function A to participating MCPTT function A3) – see example in table A.1.3-31

The non-controlling MCPTT function A invites the MCPTT user mcptt-id-A3@mcptt-op.gov to the session by sending and SIP INVITE request towards the terminating network in accordance with 3GPP TS 24.229 [4].

Table A.1.3-31: SIP INVITE request (non-Controlling MCPTT function A to participating MCPTT function A3)

```
INVITE sip: pf-A3.ims-op.net SIP/2.0
Accept-Contact:
P-Asserted-Service:
Supported:
Session-Expires:
Contact: <sessionA@cf-A2@ims-op.net61234>;g.3gpp.mcptt; isfocus; g.3gpp.icsi-ref=urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt
P-Asserted-Identity:<sip:cf-A2.ims-op.net>

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ddd:eee
m=audio 12344 RTP/AVP 97
a=
a=
a=
i=
m=application 12345 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-id-A3@mcptt-op.gov</>
    <mcptt-calling-user-id>mcptt-id-A@mcptt-op.gov</>
    <mcptt-calling-group-id>mcptt-group-T@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1--
```

Contact: Contains a new MCPTT session identity and can be used by the members to rejoin the session.

NOTE 7: The MCPTT session identity received from the controlling MCPTT function A cannot be used since when a member of group mcptt-group-A2@mcptt-op.gov rejoins the session, the member shall rejoin the session in the non-controlling MCPTT function A and not the session in the controlling MCPTT function A.

P-Asserted-Identity: Contains the public service identity of the non-controlling MCPTT function A.

mcptt-info: The identity of the invited MCPTT user mcptt-id-A3@mcptt-op.gov is added.

SDP offer: The SDP offer is a copy of the received SDP offer updated with the IP address and port numbers of the non-controlling MCPTT function A.

32) SIP INVITE request (participating MCPTT function A3 to MCPTT client A3) – see example in table A.1.3-32

The participating MCPTT function A3 sends the SIP INVITE request towards the MCPTT client A3 according to 3GPP TS 24.229 [4].

Table A.1.3-32: SIP INVITE request (participating MCPTT function A3 to MCPTT client A3)

```
INVITE sip: userA3@ims-op.net SIP/2.0
Accept-Contact:
P-Asserted-Service:
Supported:timer;tdialog
Session-Expires:refresher;uac
Contact:
Resouce-Share: media-sharing; session-receiver; rules="k3::UL"; timestamp=32651
Priority-Share:allowed
P-Asserted-Identity:<sip:cf-A2.ims-op.net>
Answer-Mode:Manual

Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:ccc:aaa:ccc
m=audio 18412 RTP/AVP 97
a=
a=
a=
i=
m=application 18413 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-request-uri>mcptt-id-A3@mcptt-op.gov</>
    <mcptt-calling-user-id>mcptt-id-A@mcptt-op.gov</>
    <mcptt-calling-group-id>mcptt-group-T@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1--
```

Request-URI: Contains the public user identity of the userA3@ims-op.net.

Resource-Share: Contains a new sharing key along with indication that MCPTT speech media can be shared in the uplink (UL) direction. The value "k3" is the key that P-CSCF can use to identify media streams towards MCPTT client A3 that can share media.

Priority-Share: The Priority-Share header field is set to "allowed" indicating that priority sharing can be applied by IMS.

Answer-Mode: The MCPTT service setting is "manual-answer" so the participating MCPTT function includes the value "Manual" in the Answer-Mode header field.

SDP offer: The SDP offer is a copy of the received SDP offer updated with the IP address and port numbers of the participating MCPTT function B.

33)-34) SIP 200 (OK) response to the SIP INVITE request (MCPTT client A3 to non-controlling MCPTT function A) – see example in table A.1.3-33

Upon receiving the SIP INVITE request the MCPTT client A3 accepts the invitation, interacts with the media plane as specified in 3GPP TS 24.380 subclause 6.2 and sends the SIP 200 (OK) response towards the MCPTT server according to rules and procedures of 3GPP TS 24.229 [4].

Table A.1.3-33: SIP 200 (OK) response (MCPTT client A3 to non-controlling MCPTT function via participating MCPTT function A3)

```
SIP/2.0 200 OK
Session-Expires:3600;refresher=uas
Require: timer
Contact:<sip:[5555::bbb:aaa:ccc:aaa]>;+g.3gpp.mcptt;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt"
P-Asserted-Identity:<sip:userA3@ims-op.net>
Supported: tdialog, norefersub, explicitsub, nosub
P-Answer-State:Confirmed
Content-Type: multipart/mixed;boundary="boundary1"
--boundary1
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::baa:abb:ddd:cccc
m=audio 25644 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=maxptime:20
i=speech
m=application 25644 udp mcptt
a=fmtp:MCPTT mc_queueing
--boundary1
Content-Type: application/vnd.3gpp.mcptt-info+xml
Content-Length: (…)

<?xml version="1.0"?>
<mcpttinfo>
  <mcptt-Params>
    <session-type>prearranged</>
    <mcptt-called-party-id>mcptt-id-A3@mcptt-op.gov</>
  </mcptt-Params>
</mcpttinfo>
--boundary1–
```

Contact: Contains the registered contact, the g.3gpp.mcptt feature tag and the g.3gpp.icsi-ref media feature tag with the IMS communication service MCPTT.

P-Answer-State: Contains the value "Confirmed" to indicate that the MCPTT client sent the response.

SDP answer: The received SDP offer is accepted and updated with the IP address and port numbers of the MCPTT client A3. The MCPTT client A3 confirms that queueing of floor requests are supported in the 'fmtp' attribute "mc_queueing".

The participating MCPTT function A3 updates the IP address and port numbers with the IP address and port numbers of the participating MCPTT function A3.

35)-36) SIP ACK request (non-controlling MCPTT function A to MCPTT client A3 via participating MCPTT function A3.

The non-controlling MCPTT function A acknowledges the receipt of the SIP 200 (OK) response to the INVITE request by means of a SIP ACK request.

37) SIP 200 (OK) response to the SIP INVITE request (non-controlling MCPTT function A to controlling MCPTT function A) – see example in table A.1.3-37

Upon receipt of the first SIP 200 (OK) response from the participating MCPTT function A3 serving the invited MCPTT user A3 in the prearranged group mcptt-id-A3@mcptt-op.gov, the non-controlling MCPTT function A interact with the media plane as specified in 3GPP TS 24.380 [5] and sends the SIP 200 (OK) towards the controlling MCPTT function A in accordance with 3GPP TS 24.229 [4].

Table A.1.3-37: SIP 200 (OK) response (non-controlling MCPTT function A to controlling MCPTT function A)

```
SIP/2.0 200 OK
Session-Expires:3600;refresher=uac
Require: timer
P-Asserted-Identity:<sip:cf-B.ims-op.net>
Contact: <sip:[5555::aaa:bbb:ddd:eee]>;+g.3gpp.mcptt;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mcptt
Supported: tdialog, norefersub, explicitsub, nosub
Content-Type: application/sdp
Content-Length: (…)

c=IN IP6 5555::aaa:bbb:ddd:eee
m=audio 12344 RTP/AVP 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=maxptime:20
i=speech
m=application 12345 udp mcptt
a=fmtp:MCPTT mc_queueing
```

P-Asserted-Identity	Contains a public service identity identifying the non-controlling MCPTT function A3.
Contact	Contains a contact address and the media feature tags g.3gpp.mcptt and g.3gpp.icsi-ref.
SDP	Contains the SDP answer to the SDP offer received from the controlling MCPTT function A. The media-level section for the media-floor control entity acknowledged that queueing is supported ("mc_queueing").

NOTE 8: The SDP answer is based on the capabilities of the non-controlling MCPTT function and not based on the SIP 200 (OK) response received from the participating MCPTT function.

38) SIP ACK request (controlling MCPTT function A to non-controlling MCPTT function A.

The controlling MCPTT function A acknowledges the receipt of the SIP 200 (OK) response to the INVITE request by means of a SIP ACK request.

Annex B (normative): Timers

B.1 General

The following tables give a brief description of the timers used in the present document.

For the on-network timers described in the present document, the following timer families are used:

- TNGx: Timer oN-network Group call x

For the off-network timers described in the present document, the following timer families are used:

- TFGx: Timer oFf-network Group call x
- TFPy: Timer oFf-network Private call y
- TFBz: Timer oFf-network Broadcast group call z

where x, y and z represent numbers.

B.2 On-network timers

B.2.1 Timers in the controlling MCPTT function

The table B.2.1-1 provides a description of the timers used by the controlling MCPTT function, specifies the timer values, describes the reason for starting of the timer, normal stop and the action on expiry.

Table B.2.1-1: controlling MCPTT function timers

Timer	Timer value	Cause of start	Normal stop	On expiry
TNG1 (acknowledged call setup timer) (NOTE 1)	Obtained from the group document in the <on-network-timeout-for-acknowledgement-of-required-members> element as specified in 3GPP TS 24.481 [31].	On reception of a SIP INVITE request to start a group session where the group document contains <on-network-required> group members as specified in 3GPP TS 24.481 [31].	On receipt of all SIP 200 (OK) responses to all SIP INVITE requests for <on-network-required> group members as specified in 3GPP TS 24.481 [31].	Either proceed with the set-up of the call or abandon the call.
TNG2 (in-progress emergency group call timer) (NOTE 2)	Obtained from the <group-time-limit> element of the <emergency-call> element of the <on-network> element of the service configuration document as specified in 3GPP TS 24.484 [50].	On reception of a SIP INVITE request or SIP re-INVITE request that initiates an MCPTT emergency group call.	On acceptance of a request to cancel the in-progress emergency state of a group.	Cancels the in-progress emergency state of the group and return the session and/or call to normal priority level.
TNG3 (group call timer). (NOTE 1).	Set to the value of the <on-network-maximum-duration> element from the group document.	On reception of a SIP INVITE request to start a group session after retrieval of the group document from the group management server. For a temporary group call, when merging active group calls into a temporary group call. When splitting a temporary group all into independent active calls	When the last MCPTT client has left the session. When a temporary group call is split into independent active calls. For active group calls, when merging them into a temporary group call.	Release the group call.
NOTE 1: More than one instance of this timer can be running in the controlling MCPTT function, each instance associated with a specific group call. NOTE 2: More than one instance of this timer can be running in the controlling MCPTT function, each instance associated with a specific in-progress emergency state of a single group				

B.3 Off-network timers

B.3.1 Timers in off-network group call

B.3.1.1 Basic call control

The table B.3.1.1-1 lists the timers used in basic call control, their start values, their limits, describes the cause of the start, and the action to take on normal stop and on expiry.

Table B.3.1.1-1: Timers in basic call control

Timer	Timer value	Cause of start	Normal stop	On expiry
TFG1 (wait for call announcement)	Default value: 150 millisecond Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFG1" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	When the client sends a CALL PROBE message.	Reception of a CALL ANNOUNCEMENT message.	Send a CALL ANNOUNCEMENT message.
TFG2 (call announcement)	Calculated. Refer to section 10.2.2.4.1.1.	Commencement of group call. Restarted every time a CALL PROBE message is received OR CALL ANNOUNCEMENT message is sent or received.	Termination of group call. When the client Receives a CALL PROBE message or CALL ANNOUNCEMENT message, Re-calculate timer value and restart.	Send a CALL ANNOUNCEMENT message. Re-calculate timer value and restart.
TFG3 (call probe retransmission)	Default value: 40 millisecond Depends on the characteristic of the D2D (D2D Sidelink period) Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFG3" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	When the client sends a CALL PROBE message.	Reception of a CALL ANNOUNCEMENT message. Or TFG1 Expires. Or User releases the call.	Send a CALL PROBE message.
TFG4 (waiting for the user)	Default value: 30 seconds Maximum value: 60 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFG4" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Reception of CALL ANNOUNCEMENT message when not participating in the ongoing call.	Reception of User action (Accept or Reject).	Stop incoming call notification.
TFG5 (not present incoming call announcements)	Default value: 30 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFG5" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Expiration of TFG4 Or User rejects the call. Or User releases the call.	-	Reset group call state machine.
TFG6 (Max duration)	Calculated. Refer to section 10.2.2.4.1.2.	Commencement of group call	Termination of group call	Release the group call

B.3.1.2 Call type control

The table B.3.1.2-1 lists the timers used in call type control, their star values, describes the cause of start, and the action to take on normal stop and on expiry.

Table B.3.1.2-1: Call type control

Timer	Timer value	Cause of start	Normal stop	On expiry
TFG11 (emergency end retransmission)	Default value: 1 second Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFG11" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	When the client sends a GROUP CALL EMERGENCY END message.	-	Send a GROUP CALL EMERGENCY END message Increment associated counter by 1. If counter has reached limit, stop the timer.
TFG12 (imminent peril end retransmission)	Default value: 1 second Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFG12" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	When the client sends a GROUP CALL IMMINENT PERIL END message.	-	Send a GROUP CALL IMMINENT PERIL END message Increment associated counter by 1. If counter has reached limit, stop the timer.
TFG13 (implicit downgrade emergency)	Calculated. Refer to subclause 10.2.3.4.1.1.	Upgrade of the call to emergency group call.	Downgrade of the call.	Downgrade the call.
TFG14 (implicit downgrade imminent peril)	Calculated. Refer to subclause 10.2.3.4.1.2.	Upgrade of the call to imminent peril call.	Downgrade of the call.	Downgrade the call.

B.3.2 Timers in off-network private call

The table B.3.2-1 lists the timers used in off-network private call, their start values, their limits, describes the cause of start, and the action to take on normal stop and on expiry.

Table B.3.2-1: Timers in off-network private call

Timer	Timer value	Cause of start	Normal stop	On expiry
TFP1 (private call request retransmission)	Default value: 40 millisecond Depends on the characteristic of the D2D (D2D Sidelink period) Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFP1" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	When the client sends a PRIVATE CALL SETUP REQUEST message.	Reception of a PRIVATE CALL ACCEPT or PRIVATE CALL REJECT message.	Resend PRIVATE CALL SETUP REQUEST message. Increment associated counter by 1. If counter has reached limit, assume the called client is not available. Terminate call setup.
TFP2 (waiting for call response message)	Default value: 30 seconds Maximum value: 60 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFP2" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Reception of a PRIVATE CALL SETUP REQUEST message.	User responds to the incoming call notification.	Start TFP7 timer. Send a PRIVATE CALL REJECT message
TFP3 (private call release retransmission)	Default value: 40 millisecond Depends on the characteristic of the D2D (D2D Sidelink period) Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFP3" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	When the client sends a PRIVATE CALL RELEASE message.	Reception of PRIVATE CALL RELEASE ACK message.	Resend PRIVATE CALL RELEASE message. Increment associated counter by 1. If counter has reached limit, assume the receiving client is not available anymore. Release the call.
TFP4 (private call accept retransmission)	Default value: 40 millisecond Depends on the characteristic of the D2D (D2D Sidelink period) Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFP4" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	When the client sends a PRIVATE CALL ACCEPT message.	Reception of a PRIVATE CALL ACCEPT ACK message or RTP media.	Resend PRIVATE CALL ACCEPT message. Increment associated counter by 1. If counter has reached limit, assume the receiving client is not available anymore Notify call setup failure.
TFP5 (max duration)	Configurable. Set to the value of "/<x>/OffNetwork/PrivateCall/MaxDuration" leaf node present in the service configuration as specified in 3GPP TS 24.483 [45].	Call establishment.	Call termination.	Terminate the call.

Timer	Timer value	Cause of start	Normal stop	On expiry
TFP6 (private emergency call cancel retransmission)	Default value: 40 millisecond Depends on the characteristic of the D2D. (D2D Sidelink period) Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFP6" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	When the client sends a PRIVATE EMERGENCY CALL CANCEL message.	Reception of a PRIVATE EMERGENCY CALL CANCEL ACK message.	Resend PRIVATE EMERGENCY CALL CANCEL message. Increment associated counter by 1. If counter has reached limit, assume the receiving client is not available anymore Notify call setup failure.
TFP7 (waiting for any message with same call identifier)	Default value: 1 second Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFP7" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Rejection of a call OR Termination of a call OR Call Failure.	-	Reset the call control state machine.
TFP8 (implicit downgrade)	Configurable. Default value: 180 seconds Set to the value of "/<x>/OffNetwork/PrivateCall/CancelTimeout" leaf node present in the service configuration as specified in 3GPP TS 24.483 [45].			

B.3.3 Timers in off-network broadcast call

The table B.3.3-1 lists the timers used in off-network broadcast call, their start values, their limits, describes the cause of start, and the action to take on normal stop and on expiry.

Table B.3.3-1: Timers in off-network broadcast call

Timer	Timer value	Cause of start	Normal stop	On expiry
TFB1 (max duration)	Default value: 300 seconds Maximum value: 600 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFB1" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Start of the broadcast call (terminating UE).	Receive GROUP CALL BROADCAST END message.	Terminate participation in the broadcast call.
TFB2 (broadcast retransmission)	Default value: 3 seconds Maximum value: 10 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFB2" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Start of the broadcast call (originating UE).	Broadcast call termination.	Send GROUP CALL BROADCAST message.
TFB3 (waiting for the user)	Default value: 30 seconds Maximum value: 60 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFB3" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Receipt of GROUP CALL BROADCAST message when user response is required.	Response from user.	Terminate incoming call notification.

B.3.4 Timers in off-network emergency alert

The table B.3.4-1 lists the timers used in off-network emergency alert, their start values, their limits, describes the cause of start, and the action to take on normal stop and on expiry.

Table B.3.4-1: Timers in off-network emergency alert

Timer	Timer value	Cause of start	Normal stop	On expiry
TFE1 (emergency alert)	Default value: 30 seconds Maximum value: 60 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFE1" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Receipt of GROUP EMERGENCY ALERT.	Receipt of GROUP EMERGENCY ALERT CANCEL.	Assume end of emergency state, remove associated user from the list.
TFE2 (emergency alert retransmission)	Default value: 5 seconds Maximum value: 10 seconds Configurable. Set to the value of "/<x>/OffNetwork/Timers/TFE2" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	Transmission of GROUP EMERGENCY ALERT.	Transmission of GROUP EMERGENCY ALERT CANCEL.	Transmit GROUP EMERGENCY ALERT.

Annex C (normative): Counters

C.1 General

The following tables give a brief description of the counters used in the present document.

C.2 Off-network counters

C.2.1 Counters in off-network group call

The table C.2.1-1 lists the counters used in off-network group call, their default upper limits and the action to take upon reaching the upper limit. The counters start at 1.

Table C.2.1-1: Counters in off-network group call

Counter	Upper Limit	Associated timer	Upon reaching the upper limit
CFG11 (emergency end retransmission)	Default value: 5 Configurable. Set to the value of "/<x>/OffNetwork/Counters/CFG11" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	TFG11	Stop timer TFG11.
CFG12 (imminent peril end retransmission)	Default value: 5 Configurable. Set to the value of "/<x>/OffNetwork/Counters/CFG12" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	TFG12	Stop timer TFG12.

C.2.2 Counters in off-network private call

The table C.2.2-1 lists the counters used in off-network private call, their default upper limits and the action to take upon reaching the upper limit. The counters start at 1.

Table C.2.2-1: Counters in off-network private call

Counter	Upper Limit	Associated timer	Upon reaching the upper limit
CFP1 (private call request retransmission)	Default value: 3 Configurable. Set to the value of "/<x>/OffNetwork/Counters/CFP1" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	TFP1	Assume the called client is not available. Terminate call setup.
CFP3 (private call release retransmission)	Default value: 3 Configurable. Set to the value of "/<x>/OffNetwork/Counters/CFP3" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	TFP3	Assume the receiving client is not available anymore. Release the call.
CFP4 (private call accept retransmission)	Default value: 3 Configurable. Set to the value of "/<x>/OffNetwork/Counters/CFP4" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	TFP4	Notify call setup failure.
CFP6 (emergency private call cancel retransmission)	Default value: 3 Configurable. Set to the value of "/<x>/OffNetwork/Counters/CFP6" leaf node present in the UE initial configuration as specified in 3GPP TS 24.483 [45].	TFP6	Notify emergency call release failure.

Annex D (normative): Media feature tags and feature-capability indicators used within the current document

D.1 General

This subclause describes the media feature tag definitions that are applicable for the 3GPP IM CN Subsystem for the realisation of the Mission Critical Push To Talk (MCPTT) service.

D.2 Definition of media feature tag g.3gpp.mcptt

Media feature tag name: g.3gpp.mcptt

Editor's Note: this media feature tag needs to be registered with IANA when the release 13 is completed.

ASN.1 Identifier: 1.3.6.1.8.2.x

Summary of the media feature indicated by this media feature tag: This media feature tag when used in a SIP request or a SIP response indicates that the function sending the SIP message supports Mission Critical Push To Talk (MCPTT) communication.

Values appropriate for use with this media feature tag: Boolean

The media feature tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This media feature tag is most useful in a communications application, for describing the capabilities of a device, such as a phone or PDA.

Examples of typical use: Indicating that a mobile phone supports the Mission Critical Push To Talk (MCPTT) communication.

Related standards or documents: 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control Protocol specification"

Security Considerations: Security considerations for this media feature tag are discussed in subclause 11.1 of IETF RFC 3840 [16].

D.3 Definition of feature-capability indicator g.3gpp.mcptt.ambient-listening-call-release

Feature-capability indicator name: g.3gpp.mcptt.ambient-listening-call-release

Summary of the feature indicated by this feature-capability indicator:

This feature-capability indicator when included in a Feature-Caps header field as specified in IETF RFC 6809 [60] in a SIP INVITE request or a SIP 200 (OK) response to a SIP INVITE request indicates that the MCPTT server is capable of receiving a SIP BYE from an MCPTT client to release an ambient-listening call.

Feature-capability indicator specification reference:

3GPP TS 24.379, http://www.3gpp.org/ftp/Specs/archive/24_series/24.379/

Values appropriate for use with this feature-capability indicator: None

Examples of typical use: Indicating that the MCPTT server can support receiving a SIP BYE from an MCPTT client to release an ambient listening call.

Security Considerations: Security considerations for this feature-capability indicator are discussed in clause 9 of IETF RFC 6809 [60].

Annex E (normative): ICSI values defined within the current document

E.1 General

This subclause describes the IMS communications service identifier definitions that are applicable for the 3GPP IM CN Subsystem for the realisation of the Mission Critical Push To Talk (MCPTT) service.

NOTE: The template has been created using the headers of the table in http://www.3gpp.org/specifications-groups/34-uniform-resource-name-urn-list

E.2 Definition of ICSI value for MCPTT service

E.2.1 URN

urn:urn-7:3gpp-service.ims.icsi.mcptt

E.2.2 Description

This URN indicates that the device has the capabilities to support the mission critical push to talk (MCPTT) service.

E.2.3 Reference

3GPP TS 24 379: "Mission Critical Push To Talk (MCPTT) call control Protocol specification"

E.2.3 Contact

Name: <MCC name>

Email: <MCC email address>

E.2.4 Registration of subtype

Yes

E.2.5 Remarks

None

Annex F (normative): XML schemas

F.1 XML schema for MCPTT Information

F.1.1 General

This subclause defines XML schema and MIME type for MCPTT information.

F.1.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:3gpp:ns:mcpttInfo:1.0"
  xmlns:mcpttinfo="urn:3gpp:ns:mcpttInfo:1.0"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:mgktp="urn:3gpp:ns:mcpttGKTP:1.0">

  <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"/>
  <xs:import namespace="urn:3gpp:ns:mcpttGKTP:1.0"/>

  <!-- root XML element -->
  <xs:element name="mcpttinfo" type="mcpttinfo:mcpttinfo-Type" id="info"/>

  <xs:complexType name="mcpttinfo-Type">
    <xs:sequence>
      <xs:element name="mcptt-Params" type="mcpttinfo:mcptt-ParamsType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcpttinfo:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="mcptt-ParamsType">
    <xs:sequence>
      <xs:element name="mcptt-access-token" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="session-type" type="xs:string" minOccurs="0"/>
      <xs:element name="mcptt-request-uri" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="mcptt-calling-user-id" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="mcptt-called-party-id" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="mcptt-calling-group-id" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="required" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="emergency-ind" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="alert-ind" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="imminentperil-ind" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="broadcast-ind" type="xs:boolean" minOccurs="0"/>
      <xs:element name="mc-org" type="xs:string" minOccurs="0"/>
      <xs:element name="floor-state" type="xs:string" minOccurs="0"/>
      <xs:element name="associated-group-id" type="xs:string" minOccurs="0"/>
      <xs:element name="originated-by" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="MKFC-GKTPs" type="mgktp:singleTypeGKTPsType" minOccurs="0"/>
      <xs:element name="mcptt-client-id" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:element name="alert-ind-rcvd" type="mcpttinfo:contentType" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcpttinfo:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:simpleType name="protectionType">
    <xs:restriction base="xs:string">
       <xs:enumeration value="Normal"/>
       <xs:enumeration value="Encrypted"/>
    </xs:restriction>
  </xs:simpleType>
```

```
  <xs:complexType name="contentType">
    <xs:choice>
      <xs:element name="mcpttURI" type="xs:anyURI"/>
      <xs:element name="mcpttString" type="xs:string"/>
      <xs:element name="mcpttBoolean" type="xs:boolean"/>
      <xs:any namespace="##other" processContents="lax"/>
      <xs:element name="anyExt" type="mcpttinfo:anyExtType" minOccurs="0"/>
    </xs:choice>
    <xs:attribute name="type" type="mcpttinfo:protectionType"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <xs:complexType name="anyExtType">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
```

F.1.3 Semantic

The <mcpttinfo> element is the root element of the XML document. The <mcpttinfo> element can contain subelements.

NOTE 1: The subelements of the <mcptt-info> are validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <mcptt-info> element

If the <mcpttinfo> contains the <mcptt-Params> element then:

1) the <mcptt-access-token>, <mcptt-request-uri>, <mcptt-calling-user-id>, <mcptt-called-party-id>, <mcptt-calling-group-id>, <emergency-ind>, <alert-ind>, <imminentperil-ind>, <originated-by> and <mcptt-client-id> can be included with encrypted content;

2) for each element in 1) that is included with content that is not encrypted:

   a) the element has the "type" attribute set to "Normal";

   b) if the element is the <mcptt-request-uri>, <mcptt-calling-user-id>, <mcptt-called-party-id> or <mcptt-calling-group-id> or <originated-by> then the <mcpttURI> element is included;

   c) if the element is the <mcptt-access-token> or <mcptt-client-id>, then the <mcpttString> element is included; and

   d) if the element is <emergency-ind>, <alert-ind>, <alert-ind-rcvd> or <imminentperil-ind> elements then the <mcpttBoolean> element is included;

3) for each element in 1) that is included with content that is encrypted:

   a) the element has the "type" attribute set to "Encrypted";

   b) the <xenc:EncryptedData> element from the "http://www.w3.org/2001/04/xmlenc#" namespace is included and:

      i) can have a "Type" attribute can be included with a value of "http://www.w3.org/2001/04/xmlenc#Content";

      ii) can include an <EncryptionMethod> element with the "Algorithm" attribute set to value of "http://www.w3.org/2009/xmlenc11#aes128-gcm";

      iii) can include a <KeyInfo> element with a <KeyName> element containing the base 64 encoded XPK-ID; and

      iv) includes a <CipherData> element with a <CipherValue> element containing the encrypted data.

NOTE 2: When the optional attributes and elements are not included within the <xenc:EncryptedData> element, the information they contain is known to sender and the receiver by other means.

If the <mcpttinfo> contains the <mcptt-Params> element then:

1) the <mcptt-access-token> can be included with the access token received during authentication procedure as described in 3GPP TS 24.482 [49];

2) the <session-type> can be included with:

   a) a value of "chat" to indicate that the MCPTT client wants to join a chat group call

   b) a value of "prearranged" to indicate the MCPTT client wants to make a prearranged group call;

   c) a value of "private" to indicate the MCPTT client wants to make a private call;

   d) a value of "first-to-answer" to indicate that the MCPTT client wants to make a first-to-answer call; or

   e) a value of "ambient-listening" to indicate the MCPTT client wants to make an ambient listening call;

3) the <mcptt-request-uri> can be included with:

   a) a value set to an MCPTT group ID or temporary MCPTT group ID when the <session-type> is set to a value of "prearranged" or "chat"; and

   b) a value set to the MCPTT ID of the called MCPTT user when the <session-type> is set to a value of "private";

4) the <mcptt-calling-user-id> can be included, set to MCPTT ID of the originating user;

5) the <mcptt-called-party-id> can be included, set to the MCPTT ID of the terminating user;

6) the <mcptt-calling-group-id> can be included to indicate the MCPTT group identity to the terminating user;

7) the <required> can be included in a SIP 183 (Session Progress) from a non-controlling MCPTT function of an MCPTT group to inform the controlling MCPTT function that the group on the non-controlling MCPTT function has group members in the group document which are marked as <on-network-required>, as specified in 3GPP TS 24.481 [31];

8) the <emergency-ind> can be:

   a) set to "true" to indicate that the call that the MCPTT client is initiating is an emergency MCPTT call; or

   b) set to "false" to indicate that the MCPTT client is cancelling an emergency MCPTT call (i.e. converting it back to a non-emergency call)

9) the <alert-ind> can be:

   a) set to "true" in an emergency call initiation to indicate that an alert to be sent; or

   b) set to "false" when cancelling an emergency call which requires an alert to be cancelled also

10) if the <session-type> is set to "chat" or "prearranged":

   a) the <imminentperil-ind> can be set to "true" to indicate that the call that the MCPTT client is initiating is an imminent peril group MCPTT call;

11) the <broadcast-ind> can be:

   a) set to "true" indicates that the MCPTT client is initiating a broadcast group call; or

   b) set to "false" indicates that the MCPTT client is initiating a non-broadcast group call;

12) the <mc-org> can be:

   a) set to the MCPTT user's Mission Critical Organization in an emergency alert sent by the MCPTT server to terminating MCPTT clients;

13) the <floor-state> can be:

   a) set to "floor-idle", if the floor is idle in a non-controlling MCPTT function; or

   b) set to "floor-taken" if the floor state in a non-controlling MCPTT function is taken;

14) the <associated-group-id>:

   a) if the <mcptt-request-uri> element contains a group identity then this element can include an MCPTT group ID associated with the group identity in the <mcptt-request-uri> element. E.g. if the <mcptt-request-uri> element contains a temporary group identity (TGI), then the <associated-group-id> element can contain the constituent MCPTT group ID;

15) the <originated-by>:

   a) can be included, set to the MCPTT ID of the originating user of an MCPTT emergency alert when being cancelled by another authorised MCPTT user;

16) the <MKFC-GKTPs>:

   a) contains a group key transport payload carrying one or more MKFC(s) and MKFC-ID(s) as described in3GPP TS 24.481 [31] subclause 7.4, to be used for protection of multicast floor control signalling when the UE operates on the network;

17) the <mcptt-client-id>:

   a) can be included, set to the MCPTT client ID of the MCPTT client that originated a SIP INVITE request, SIP REFER request or SIP MESSAGE request;

18) the <alert-ind-rcvd>

   a) can be set to true and included in a SIP MESSAGE to indicate that the emergency alert or cancellation was received successfully; and

19) the <anyExt> can be included with the following elements not declared in the XML schema:

   a) an <ambient-listening-type> of type "xs:string":

      i) set to a value of "remote-init" when the listening MCPTT user of an ambient listening call initiates the call; or

      ii) set to a value of "local-init" when the listened-to MCPTT user of an ambient listening call initiates the call; and

   b) a <release-reason> of type "xs:string":

      i) set to a value of "private-call-expiry" when the ambient listening call is release due to the expiry of the private call timer;

      ii) set to a value of "administrator-action" when the ambient listening call is released by an MCPTT administrator;

      iii) set to a value of "not selected for call" when the when a dialog is released with an MCPTT client that was not selected as the terminating client of a first-to-answer call;

      iv) set to a value of "call-request-for-listened-to-client" when there is a call request targeted to the listened-to client;

      v) set to a value of "call-request-initiated-by-listened-to-client" when there is a call request initiated by the listened-to client; or

      vi) set to a value of "authentication of the MIKEY-SAKE I_MESSAGE failed" by a MCPTT client when the signature of the cannot be verified;

   c) a <request-type> of type "xs:string":

      i) set to value of "private-call-call-back-request" when a client initiates a private call call-back request;

      ii) set to a value of "private-call-call-back-cancel-request" when a client initiates a private call call-back cancel request; or

      iii) set to a value of "group-selection-change-request" when a client initiates a group selection change request;

d) a <response-type> of type "xs:string":

i) set to a value of "private-call-call-back-response" when a client responds to a private call call-back request; or

ii) set to a value of "private-call-call-back-cancel-response" when a client responds to a private call call-back cancel request; or

iii) set to a value of "group-selection-change-response" when a client responds to a group selection change request;

e) an <urgency indication> of type "xs:string":

(i) set to a value of "low", "normal" or "high" to indicate the urgency of a private call call-back request; and

f) a <time-of-request> of type "xs:dateTime":

(i) set to the date and time at which the private call call-back request was initiated, in the form: "YYYY-MM-DDThh:mm:ss" where:

- YYYY indicates the year;
- MM indicates the month;
- DD indicates the day;
- T indicates the start of the required time section;
- hh indicates the hour;
- mm indicates the minute; and
- ss indicates the second; and

g) a <selected-group-change-outcome> of type "xs:string":

i) set to a value of "success" when a client reports that it has successfully changed its selected group as requested by a received group selection change request; or

ii) set to a value of "fail" when a client reports that it has failed to change its selected group as requested by a received group selection change request; and

h) an<affiliation-required> of type "xs:Boolean":

i) set to a value of "true" when received by a client in a group-selection-change-request indicates that the client needs to affiliate to the specified group.

Absence of the <emergency-ind>, <alert-ind> and <imminentperil-ind> in a SIP INVITE request indicates that the MCPTT client is initiating a non-emergency private call or non-emergency group call.

Absence of the <broadcast-ind> in a SIP INVITE request indicates that the MCPTT client is initiating a non-broadcast group call.

Absence of the <floor-state> in a SIP 200 (OK) response from the non-controlling MCPTT function indicates that the floor is idle.

The recipient of the XML ignores any unknown element and any unknown attribute.

F.1.4 IANA registration template

Editor's note [CT1#95, C1-154478]: The MIME type application/vnd.3gpp.mcptt-info +xml as defined in this subclause is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcptt-info+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.379 "Mission Critical Push To Talk (MCPTT) call control" version 13.0.0, available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical push to talk as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
  i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG
  ii) Change controller: <MCC name>/<MCC email address>

F.2 XML schema for MBMS usage information

F.2.1 General

This subclause defines XML schema and MIME type for application/vnd.3gpp.mcptt-mbms-usage-info+xml.

F.2.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:3gpp:ns:mcpttMbmsUsage:1.0"
xmlns:mcpttmbms="urn:3gpp:ns:mcpttMbmsUsage:1.0">
    <!-- the root element -->
    <xs:element name="mcptt-mbms-usage-info" type="mcpttmbms:mcptt-mbms-usage-info-Type" id="mbms"/>
    <xs:complexType name="mcptt-mbms-usage-info-Type">
        <xs:sequence>
            <xs:element name="mbms-listening-status" type="mcpttmbms:mbms-listening-statusType"
            minOccurs="0"/>
            <xs:element name="mbms-suspension-status" type="mcpttmbms:mbms-suspension-statusType"
            minOccurs="0"/>
            <xs:element name="announcement" type="mcpttmbms:announcementTypeParams" minOccurs="0"/>
            <xs:element name="version" type="xs:integer"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttmbms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="mbms-listening-statusType">
        <xs:sequence>
            <xs:element name="mbms-listening-status" type="xs:string"/>
            <xs:element name="session-id" type="xs:anyURI" minOccurs="0"/>
            <xs:element name="general-purpose" type="xs:boolean" minOccurs="0"/>
            <xs:element name="TMGI" type="xs:hexBinary" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
```

```
            <xs:element name="anyExt" type="mcpttmbms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="mbms-suspension-statusType">
        <xs:sequence>
            <xs:element name="mbms-suspension-status" type="xs:string" minOccurs="0" maxOccurs="1"/>
            <xs:element name="number-of-reported-bearers" type="xs:integer" minOccurs="0"
maxOccurs="1"/>
            <xs:element name="suspended-TMGI" type="xs:hexBinary" minOccurs="0"/>
            <xs:element name="other-TMGI" type="xs:hexBinary" minOccurs="0" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttmbms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:element name="mbms-defaultMuSiK-download" type="mcpttmbms:mbms-default-ctrlkey-
downloadType"/>
<xs:complexType name="mbms-default-ctrlkey-downloadType">
        <xs:sequence>
            <xs:element type="xs:anyURI" name="group" minOccurs="0" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttmbms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:element name="mbms-explicitMuSiK-download" type="mcpttmbms:mbms-explicit-ctrlkey-
downloadType"/>
    <xs:complexType name="mbms-explicit-ctrlkey-downloadType">
        <xs:sequence>
            <xs:element type="xs:anyURI" name="group" minOccurs="1" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttmbms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="announcementTypeParams">
        <xs:sequence>
            <xs:element name="TMGI" type="xs:hexBinary" minOccurs="1"/>
            <xs:element name="QCI" type="xs:integer" minOccurs="0"/>
            <xs:element name="frequency" type="xs:unsignedLong" minOccurs="0"/>
            <xs:element name="mbms-service-areas" type="xs:hexBinary" minOccurs="0"/>
            <xs:element name="GPMS" type="xs:positiveInteger" minOccurs="0"/>
            <xs:element name="report-suspension" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttmbms:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="anyExtType">
        <xs:sequence>
            <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

F.2.3 Semantic

This subclause describes the elements of the MBMS usage information XML Schema.

<mbms-listening-status>: The <mbms-listening-status> element is used to indicate the MCPTT listening status.

- The value "listening" indicates that the MCPTT client now is receiving RTP media packets and floor control messages over the MBMS subchannel in the session identified by the <session-id> element or if the <general-purpose> element is set to "true", that the MCPTT client is now listening to the general purpose MBMS subchannel.

- The value "not-listening" indicates that the MCPTT client has stopped listening to the MBMS subchannel in the session identified by the <session-id> element or, if the <general-purpose> element is set to "false", that the MCPTT client no longer listens to the general purpose MBMS subchannel.

Table F.2.3-1 shows the ABNF of the <mbms-listening-status> element.

Table F.2.3-1: ABNF syntax of values of the <mbms-listening-status> element

```
mbms-listening-status = listening-value / not-listening-value
listening-value = %x6c.69.73.74.65.6e.69.6e.67 ; "listening"
not-listening-value = %x6e.6f.74.2d.6c.69.73.74.65.6e.69.6e.67 ; "not-listening"
```

<session-id>: contains the value of the URI received in the Contact header field received from the controlling MCPTT function when an on-demand session was established, or from the participating MCPTT function in the Connect message when the session was established over a pre-established session. This element is mandatory if the <general-purpose> element is not present in the application/vnd.3gpp.mcptt-mbms-usage-info+xml MIME body.

<TMGI>: Contains the TMGI. The <TMGI> element is coded as described in 3GPP TS 24.008 [43] subclause 10.5.6.13 excluding the Temporary Mobile Group Identity IEI and Length of Temporary Mobile Group Identity contents (octet 1 and octet 2 in 3GPP TS 24.008 [43] subclause 10.5.6.13).

<QCI>: QCI information used by the ProSe UE-Network Relay to determine the ProSe Per-Packet Priority value to be applied for the multicast packets relayed to Remote UE over PC5. QCI values are defined in 3GPP TS 23.203 [41].

<mbms-service-areas>: A list of MBMS service area IDs for the applicable MBMS broadcast area as specified in 3GPP TS 23.003 [40] for Service Area Identifier (SAI), and with the encoding as specified in 3GPP TS 29.061 [74] for the MBMS-Service-Area AVP.

<Frequency>: Identification of frequency in case of multi carrier support. The <Frequency> element is coded as specified in 3GPP TS 29.468 [42].

NOTE 1: In the current release the frequency in the <frequency> element is the same as the frequency used for unicast.

<SDP-ref>: A URL with a cid url as specified in IETF RFC 5368 [38] referring to a SDP MIME body in the SIP MESSAGE request.

<general-purpose> True indicates that the MCPTT client is listening to the general purpose MBMS subchannel associated to the TMGI(s) in the <TMGI> element(s) but have not yet received a Map Group To bearer message for any session that the MCPTT client is involved in. False indicates that the MCPTT client is not listening to the general purpose MBMS subchannel any longer. Absence of the element requires that the <session-id> element is present in the application/vnd.3gpp.mcptt-mbms-usage-info+xml.

<GPMS> A positive integer that gives the number of the media line containing the general purpose MBMS subchannel in the application/sdp MIME body attached to the SIP MESSAGE request containing the MBMS announcements.

<version> this element indicates the version of the application/vnd.3gpp.mbms-usage-info MIME body. In this version the <version element> indicates "1".

<report-suspension>:True indicates that the MCPTT client is instructed to notify the MCPTT server when it becomes aware of an intended change in the suspension status of a listened MBMS bearer. False indicates that the MCPTT client is instructed not to notify the MCPTT server if it becomes aware of an intended change in the suspension status of a listened MBMS bearer.

<mbms-suspension-status>: The <mbms-suspension-status> element is used to indicate the MBMS bearers intended suspension status.

- The value "suspending" indicates that the RAN has decided to suspend the referenced MBMS bearer(s) at the beginning of the next MCCH modification period .
- The value "not-suspending" indicates that the RAN has decided to revoke its decision to suspend the referenced MBMS bearer(s) before the beginning of the next MCCH modification period.

Table F.2.3-2 shows the ABNF of the <mbms-suspension-status> element.

Table F.2.3-2: ABNF syntax of values of the <mbms-suspension-status> element

```
mbms-suspension-status = suspending-value / not-suspending-value
suspending-value = %x73.75.73.70.65.6e.64.69.6e.67 ; "suspending"
not-suspending-value = %x6e.6f.74.2d.73.75.73.70.65.6e.64.69.6e.67 ; "not-suspending"
```

<number-of-reported-bearers>: the total number of occurrences of the <suspended-TMGI> and <other-TMGI> elements reported as part of the MBMS bearer suspension status.

<suspended-TMGI>:Contains a TMGI that is being reported as about to be suspended or as no longer about to be suspended.

<other-TMGI>: Contains a TMGI that is not being reported as about to be suspended or as no longer about to be suspended, but which shares the same MCH with MBMS bearers reported in the <suspended-TMGI> elements.

<mbms-defaultMuSiK-download> is included in <anyExt> element of the <mcptt-mbms-usage-info-Type> element and provides information for default MuSiK download.

NOTE 2: When included, the <mbms-defaultMuSiK-download> element is validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <anyExt> element.

<mbms-explicitMuSiK-download>is included in <anyExt> element of the <mcptt-mbms-usage-info-Type> element and provides information for explicit MuSiK download.

NOTE 3: When included, the <mbms-explicitMuSiK-download> element is validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <anyExt> element.

<group>: Contains the identity, in the form of a URI, of a group for which the MuSiK download is performed.

The recipient of the XML ignores any unknown element and any unknown attribute.

F.2.4 IANA registration template

Editor's note [CT1#95-bis, C1-160397]: The MIME type application/vnd.3gpp.mcptt-mbms-usage-info+xml as defined in this subclause is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcptt-mbms-usage-info+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.379 "Mission Critical Push To Talk (MCPTT) call control" version 13.0.0, available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical push to talk as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
  i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG
  ii) Change controller: <MCC name>/<MCC email address>

F.3 XML schema for MCPTT location information

F.3.1 General

This subclause defines the XML schema and the MIME type for location information.

F.3.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:mcpttloc="urn:3gpp:ns:mcpttLocationInfo:1.0"
targetNamespace="urn:3gpp:ns:mcpttLocationInfo:1.0" elementFormDefault="qualified"
attributeFormDefault="unqualified"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

    <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"/>

    <xs:element name="location-info" id="loc">
        <xs:annotation>
            <xs:documentation>Root element, contains all information related to location
configuration, location request and location reporting for the MCPTT service</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:choice>
                <xs:element name="Configuration" type="mcpttloc:tConfigurationType"/>
                <xs:element name="Request" type="mcpttloc:tRequestType"/>
                <xs:element name="Report" type="mcpttloc:tReportType"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
            </xs:choice>
            <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="tConfigurationType">
        <xs:sequence>
            <xs:element name="NonEmergencyLocationInformation"
type="mcpttloc:tRequestedLocationType" minOccurs="0"/>
            <xs:element name="EmergencyLocationInformation" type="mcpttloc:tRequestedLocationType"
minOccurs="0"/>
            <xs:element name="TriggeringCriteria" type="mcpttloc:TriggeringCriteriaType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="ConfigScope">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Full"/>
                    <xs:enumeration value="Update"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tRequestType">
        <xs:complexContent>
            <xs:extension base="mcpttloc:tEmptyType">
                <xs:attribute name="RequestId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:complexContent>
```

```
    </xs:complexType>
    <xs:complexType name="tReportType">
        <xs:sequence>
            <xs:element name="TriggerId" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="CurrentLocation" type="mcpttloc:tCurrentLocationType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="ReportID" type="xs:string" use="optional"/>
        <xs:attribute name="ReportType" use="required">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Emergency"/>
                    <xs:enumeration value="NonEmergency"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="TriggeringCriteriaType">
        <xs:sequence>
            <xs:element name="CellChange" type="mcpttloc:tCellChange" minOccurs="0"/>
            <xs:element name="TrackingAreaChange" type="mcpttloc:tTrackingAreaChangeType"
minOccurs="0"/>
            <xs:element name="PlmnChange" type="mcpttloc:tPlmnChangeType" minOccurs="0"/>
            <xs:element name="MbmsSaChange" type="mcpttloc:tMbmsSaChangeType" minOccurs="0"/>
            <xs:element name="MbsfnAreaChange" type="mcpttloc:tMbsfnAreaChangeType" minOccurs="0"/>
            <xs:element name="PeriodicReport" type="mcpttloc:tIntegerAttributeType" minOccurs="0"/>
            <xs:element name="TravelledDistance" type="mcpttloc:tIntegerAttributeType"
minOccurs="0"/>
            <xs:element name="McpttSignallingEvent" type="mcpttloc:tSignallingEventType"
minOccurs="0"/>
            <xs:element name="GeographicalAreaChange" type="mcpttloc:tGeographicalAreaChange"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tCellChange">
        <xs:sequence>
            <xs:element name="AnyCellChange" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificCell" type="mcpttloc:tSpecificCellType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="ExitSpecificCell" type="mcpttloc:tSpecificCellType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEmptyType"/>
    <xs:simpleType name="tEcgi">
        <xs:restriction base="xs:string">
            <xs:pattern value="\d{3}\d{3}[0-1]{28}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tSpecificCellType">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tEcgi">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tEmptyTypeAttribute">
        <xs:complexContent>
            <xs:extension base="mcpttloc:tEmptyType">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="tTrackingAreaChangeType">
        <xs:sequence>
            <xs:element name="AnyTrackingAreaChange" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="EnterSpecificTrackingArea" type="mcpttloc:tTrackingAreaIdentity"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="ExitSpecificTrackingArea" type="mcpttloc:tTrackingAreaIdentity"
minOccurs="0" maxOccurs="unbounded"/>
```

```
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tTrackingAreaIdentityFormat">
        <xs:restriction base="xs:string">
            <xs:pattern value="\d{3}\d{3}[0-1]{16}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tTrackingAreaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tTrackingAreaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tPlmnChangeType">
        <xs:sequence>
            <xs:element name="AnyPlmnChange" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificPlmn" type="mcpttloc:tPlmnIdentity" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="ExitSpecificPlmn" type="mcpttloc:tPlmnIdentity" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tPlmnIdentityFormat">
        <xs:restriction base="xs:string">
            <xs:pattern value="\d{3}\d{3}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tPlmnIdentity">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tPlmnIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tMbmsSaChangeType">
        <xs:sequence>
            <xs:element name="AnyMbmsSaChange" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificMbmsSa" type="mcpttloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:element name="ExitSpecificMbmsSa" type="mcpttloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tMbmsSaIdentityFormat">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="65535"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tMbmsSaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tMbmsSaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tMbsfnAreaChangeType">
        <xs:sequence>
            <xs:element name="EnterSpecificMbsfnArea" type="mcpttloc:tMbsfnAreaIdentity"
minOccurs="0"/>
            <xs:element name="ExitSpecificMbsfnArea" type="mcpttloc:tMbsfnAreaIdentity"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tMbsfnAreaIdentityFormat">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
```

```
            <xs:maxInclusive value="255"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tMbsfnAreaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tMbsfnAreaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tIntegerAttributeType">
        <xs:simpleContent>
            <xs:extension base="xs:integer">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tTravelledDistanceType">
        <xs:sequence>
            <xs:element name="TravelledDistance" type="xs:positiveInteger"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tSignallingEventType">
        <xs:sequence>
            <xs:element name="InitialLogOn" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="GroupCallNonEmergency" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="PrivateCallNonEmergency" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="LocationConfigurationReceived" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type=" mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEmergencyEventType">
        <xs:sequence>
            <xs:element name="GroupCallEmergency" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="GroupCallImminentPeril" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="PrivateCallEmergency" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="InitiateEmergencyAlert" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tRequestedLocationType">
        <xs:sequence>
            <xs:element name="ServingEcgi" type="mcpttloc:tEmptyType" minOccurs="0"/>
            <xs:element name="NeighbouringEcgi" type="mcpttloc:tEmptyType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="MbmsSaId" type="mcpttloc:tEmptyType" minOccurs="0"/>
            <xs:element name="MbsfnArea" type="mcpttloc:tEmptyType" minOccurs="0"/>
            <xs:element name="GeographicalCordinate" type="mcpttloc:tEmptyType" minOccurs="0"/>
            <xs:element name="minimumIntervalLength" type="xs:positiveInteger"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tCurrentLocationType">
        <xs:sequence>
            <xs:element name="CurrentServingEcgi" type="mcpttloc:tLocationType" minOccurs="0"/>
            <xs:element name="NeighbouringEcgi" type="mcpttloc:tLocationType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="MbmsSaId" type="mcpttloc:tLocationType" minOccurs="0"/>
            <xs:element name="MbsfnArea" type="mcpttloc:tLocationType" minOccurs="0"/>
            <xs:element name="CurrentCoordinate" type="mcpttloc:tPointCoordinate" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
```

```
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:simpleType name="protectionType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Normal"/>
            <xs:enumeration value="Encrypted"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="tLocationType">
        <xs:choice minOccurs="1" maxOccurs="1">
            <xs:element name="Ecgi" type="mcpttloc:tEcgi" minOccurs="0"/>
            <xs:element name="SaId" type="mcpttloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:element name="MbsfnAreaId" type="mcpttloc:tMbsfnAreaIdentity" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"/>
            <xs:element name="anyExt" type="mcpttinfo:anyExtType" minOccurs="0"/>
        </xs:choice>
        <xs:attribute name="type" type="protectionType"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tGeographicalAreaChange">
        <xs:sequence>
            <xs:element name="AnyAreaChange" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificAreaType" type="mcpttloc:tSpecificAreaType"
minOccurs="0"/>
            <xs:element name="ExitSpecificAreaType" type="mcpttloc:tSpecificAreaType"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tSpecificAreaType">
        <xs:sequence>
            <xs:element name="GeographicalArea" type="mcpttloc:tGeographicalAreaDef"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="TriggerId" type="xs:string" use="required"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tPointCoordinate">
        <xs:sequence>
            <xs:element name="longitude" type="mcpttloc:tCoordinateType"/>
            <xs:element name="latitude" type="mcpttloc:tCoordinateType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tCoordinateType">
        <xs:choice minOccurs="1" maxOccurs="1">
            <xs:element name="threebytes" type="mcpttloc:tThreeByteType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"/>
            <xs:element name="anyExt" type="mcpttinfo:anyExtType" minOccurs="0"/>
        </xs:choice>
        <xs:attribute name="type" type="protectionType"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:simpleType name="tThreeByteType">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="16777215"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tGeographicalAreaDef">
        <xs:sequence>
            <xs:element name="PolygonArea" type="mcpttloc:tPolygonAreaType" minOccurs="0"/>
            <xs:element name="EllipsoidArcArea" type="mcpttloc:tEllipsoidArcType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
```

```
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tPolygonAreaType">
        <xs:sequence>
            <xs:element name="Corner" type="mcpttloc:tPointCoordinate" minOccurs="3"
maxOccurs="15"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEllipsoidArcType">
        <xs:sequence>
            <xs:element name="Center" type="mcpttloc:tPointCoordinate"/>
            <xs:element name="Radius" type="xs:nonNegativeInteger"/>
            <xs:element name="OffsetAngle" type="xs:unsignedByte"/>
            <xs:element name="IncludedAngle" type="xs:unsignedByte"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="anyExtType">
        <xs:sequence>
            <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

F.3.3 Semantic

The <location-info> element is the root element of the XML document. The <location-info> element contains the <Configuration>, <Request> and <Report> subelements, of which only one can be present.

<Configuration> element has a <ConfigScope> attribute that can assume the values "Full" and "Update". The value "Full" means that the Configuration> element contains the full location configuration which replaces any previous location configuration. The value "Update" means that the location configuration is in addition to any previous location configuration. To remove configuration elements a "Full" configuration is needed. The <Configuration> element contains the following child elements:

1) <NonEmergencyLocationInformation>, an optional element that specifies the location information requested in non-emergency situations. The <NonEmergencyLocationInformation> has the subelements:

   a) <ServingEcgi>, an optional element specifying that the serving E-UTRAN Cell Global Identity (ECGI) needs to be reported;

   b) <NeighbouringEcgi>, an optional element that can occur multiple times, specifying that neighbouring ECGIs need to be reported;

   c) <MbmsSaId>, an optional element specifying that the serving MBMS Service Area Id needs to be reported;

   d) <MbsfnArea>, an optional element specifying that the MBSFN area Id needs to be reported;

   e) <GeographicalCoordinate>, an optional element specifying that the geographical coordinate specified in subclause 6.1 in 3GPP TS 23.032 [54] needs to be reported; and

   f) <minimumIntervalLength>, a mandatory element specifying the minimum time the MCPTT client needs to wait between sending location reports. The value is given in seconds;

2) <EmergencyLocationInformation>, an optional element that specifies the location information requested in emergency situations. The <EmergencyLocationInformation> has the subelements:

   a) <ServingEcgi>, an optional element specifying that the serving ECGI needs to be reported;

   b) <NeighbouringEcgi>, an optional element that can occur multiple times, specifying that neighbouring ECGIs need to be reported;

   c) <MbmsSaId>, an optional element specifying that the serving MBMS Service Area Id needs to be reported;

d) <MbsfnArea>, an optional element specifying that the MBSFN area Id needs to be reported;

e) <GeographicalCoordinate>, an optional element specifying that the geographical coordinate specified in subclause 6.1 in 3GPP TS 23.032 [54] needs to be reported; and

f) <minimumIntervalLength>, a mandatory element specifying the minimum time the MCPTT client needs to wait between sending location reports. The value is given in seconds; and

3) <TriggeringCriteria>, a mandatory element specifying the triggers for the MCPTT client to perform reporting. The <TriggeringCriteria> element contains the following sub-elements:

a) <CellChange>, an optional element specifying what cell changes trigger location reporting. Consists of the following sub-elements:

I) <AnyCellChange>, an optional element. The presence of this element specifies that any cell change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <EnterSpecificCell>, an optional element specifying an ECGI which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

III) <ExitSpecificCell>, an optional element specifying an ECGI which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

b) <TrackingAreaChange>, an optional element specifying what tracking area changes trigger location reporting. Consists of the following sub-elements:

I) <AnyTrackingAreaChange>, an optional element. The presence of this element specifies that any tracking area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <EnterSpecificTrackingArea>, an optional element specifying a Tracking Area Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

III) <ExitSpecificTrackingArea>, an optional element specifying a Tracking Area Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

c) <PlmnChange>, an optional element specifying what PLMN changes trigger location reporting. Consists of the following sub-elements:

I) <AnyPlmnChange>, an optional element. The presence of this element specifies that any PLMN change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <EnterSpecificPlmn>, an optional element specifying a PLMN Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

III) <ExitSpecificPlmn>, an optional element specifying a PLMN Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

d) <MbmsSaChange>, an optional element specifying what MBMS changes trigger location reporting. Consists of the following sub-elements:

I) <AnyMbmsSaChange>, an optional element. The presence of this element specifies that any MBMS SA change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <EnterSpecificMbmsSa>, an optional element specifying an MBMS Service Area Id which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

III) <ExitSpecificMbmsSa>, an optional element specifying an MBMS Service Area Id which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

e) <MbsfnAreaChange>, an optional element specifying what MBSFN changes trigger location reporting. Consists of the following sub-elements:

I) <AnyMbsfnAreaChange>, an optional element. The presence of this element specifies that any MBSFN area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <EnterSpecificMbsfnArea>, an optional element specifying an MBSFN area which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

III) <ExitSpecificMbsfnArea>, an optional element specifying an MBSFN area which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

f) <PeriodicReport>, an optional element specifying that periodic location reports shall be sent. The value in seconds specifies the reporting interval. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

g) <TravelledDistance>, an optional element specifying that the travelled distance shall trigger a report. The value in metres specified the travelled distance. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

h) <McpttSignallingEvent>, an optional element specifying what signalling events triggers a location report. The <McpttSignallingEvent> element has the following sub-elements:

I) <InitialLogOn>, an optional element specifying that an initial log on triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <GroupCallNonEmergency>, an optional element specifying that a non-emergency group call triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

III) <PrivateCallNonEmergency>, an optional element specifying that a non-emergency private call triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

IV) <LocationConfigurationReceived>, an optional element specifying that a received location configuration triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string; and

i) <GeographicalAreaChange>, an optional element specifying what geographical are changes trigger location reporting. Consists of the following sub-elements:

I) <AnyAreaChange>, an optional element. The presence of this element specifies that any geographical area change is a trigger. Contains a mandatory <TriggerId> attribute that shall be set to a unique string;

II) <EnterSpecificArea>, an optional element specifying a geographical area which when entered triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string. The <EnterSpecificArea> element has the following sub-elements:

A) <GeographicalArea>, an optional element containing a <TriggerId> attribute and the following two subelements:

x1) <PolygonArea>, an optional element specifying the area as a polygon specified in subclause 5.2 in 3GPP TS 23.032 [54]; and

x2) <EllipsoidArcArea>, an optional element specifying the area as an Ellipsoid Arc specified in subclause 5.7 in 3GPP TS 23.032 [54]; and

III) <ExitSpecificAreaType>, an optional element specifying a geographical area which when exited triggers a location report. Contains a mandatory <TriggerId> attribute that shall be set to a unique string.

<Request> is an element with a <RequestId> attribute. The <Request> element is used to request a location report. The value of the <RequestId> attribute is returned in the corresponding <ReportId> attribute in order to correlate the request and the report.

<Report> is an element used to include the location report. It contains a <ReportId> attribute and a <ReportType> attribute. The <ReportId> attribute is used to return the value in the <RequestId> attribute in the <Request> element. The <ReportType> attribute has two values "Emergency" and "NonEmergency" used to inform whether the client is sending the report in an emergency situation or not. The <Report> element contains the following sub-elements:

1) <TriggerId>, an optional element which can occur multiple times that contain the value of the <TriggerId> attribute associated with a trigger that has fired; and

2) <CurrentLocation>, a mandatory element that contains the location information. The <CurrentLocation> element contains the following sub-elements:

   a) <CurrentServingEcgi>, an optional element containing the ECGI of the serving cell;

   b) <NeighbouringEcgi>, an optional element that can occur multiple times. It contains the ECGI of any neighbouring cell the MCPTT client can detect;

   c) <MbmsSaId>, an optional element containing the MBMS Service Area Id the MCPTT client is using;

   d) <MbsfnArea>, an optional element containing the MBSFN area the MCPTT is located in; and

   e) <CurrentCoordinate>, an optional element containing the longitude and latitude coded as in subclause 6.1 in 3GPP TS 23.032 [54].

The contents of the subelements in the <CurrentLocation> subelement of the <Report> element can be encrypted. The following rules are applied when any of these elements are included:

1) if confidentiality protection is not required, then:

   a) the "type" attributes associated with the <CurrentServingEcgi>, <NeighbouringEcgi>, <MbmsSaId>, and <MbsfnArea> elements of the <Report> element have the value "Normal" and

      ii) the <Ecgi> subelement of the <CurrentServingEcgi> element contains the unencrypted value of the ECGI of the serving cell;

      iii) the <Ecgi> subelement of the <NeighbouringEcgi> element contains the unencrypted value of the ECGI of any neighbouring cell;

      iv) the <SaId> subelement of the <MbmsSaId> element contains the unencrypted value of the MBMS Service Area Id the MCPTT client is using; and

      v) the <MbsfnAreaId> subelement of the <MbsfnArea>, element contains the unencrypted value of the MBSFN area the MCPTT is located in;

   b) the "type" attributes associated with the <longitude> and <latitude> subelements of the <CurrentCoordinate> element have the value "Normal" and the <three-bytes> subelements of <longitude> and <latitude> subelements contain the unencrypted value of longitude and latitude.

2) if confidentiality protection is required, then:

   a) the "type" attributes associated with the <CurrentServingEcgi>, <NeighbouringEcgi>, <MbmsSaId>, and <MbsfnArea> elements have the value "Encrypted";

   b) the "type" attributes associated with the <longitude> and <latitude> subelements of the <CurrentCoordinate> element have the value "Encrypted";

   c) for each of the elements described in 2a) and subelements described in 2b) above, the <xenc:EncryptedData> element from the "http://www.w3.org/2001/04/xmlenc#" namespace is included and:

      i) can have a "Type" attribute can be included with a value of "http://www.w3.org/2001/04/xmlenc#Content";

      ii) can include an <EncryptionMethod> element with the "Algorithm" attribute set to value of "http://www.w3.org/2009/xmlenc11#aes128-gcm";

      iii) can include a <KeyInfo> element with a <KeyName> element containing the base 64 encoded XPK-ID; and

      iv) includes a <CipherData> element with a <CipherValue> element containing the encrypted data.

NOTE: When the optional attributes and elements are not included within the <xenc:EncryptedData> element, the information they contain is known to sender and the receiver by other means.

The recipient of the XML ignores any unknown element and any unknown attribute.

F.3.4 IANA registration template

Editor's note [CT1#95-bis, C1-160453]: The application/vnd.3gpp.mcptt-location-info+xml MIME type as defined in this subclause needs to be registered at completion of Release-13.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp. mcptt-location-info+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.379 "Mission Critical Push To Talk (MCPTT) call control" version 13.0.0, available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical push to talk as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
  i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG
  ii) Change controller: <MCC name>/<MCC email address>

F.4 XML schema for MCPTT (de)-affiliation requests

F.4.1 General

This subclause defines XML schema and MIME type for MCPTT (de)-affiliation requests.

F.4.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:3gpp:ns:affiliationCommand:1.0"
xmlns:mcpttaff="urn:3gpp:ns:affiliationCommand:1.0"
attributeFormDefault="unqualified" elementFormDefault="qualified">
  <xs:complexType name="affiliate-command" id="affil">
    <xs:sequence>
      <xs:element type="xs:anyURI" name="group" minOccurs="1" maxOccurs="unbounded"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcpttaff:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>
  <xs:complexType name="de-affiliate-command">
    <xs:sequence>
      <xs:element type="xs:anyURI" name="group" minOccurs="1" maxOccurs="unbounded"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcpttaff:anyExtType" minOccurs="0"/>
```

```
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>
  <xs:element name="command-list">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="affiliate" type="mcpttaff:affiliate-command" minOccurs="0" maxOccurs="1"/>
        <xs:element name="de-affiliate" type="mcpttaff:de-affiliate-command" minOccurs="0"
maxOccurs="1"/>
        <xs:element name="anyExt" type="mcpttaff:anyExtType" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="anyExtType">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

F.4.3 Semantic

The <command-list> element is the root element of the XML document. The <command-list> element may contain <affiliate-command>, or <de-affiliate-command> subelements or both.

If the <command-list> contains the <affiliate-command> element then:

1) the <affiliate-command> element contains a list of <group> subelements having at least one subelement. The recipient shall perform an affiliation for all the MCPTT groups contained in the list for the clients for which the <command-list> applies.

If the <command-list> contains the <de-affiliate-command> element then:

1) the <de-affiliate-command> element contains a list of <group> subelements having at least one subelement. The recipient shall perform a de-affiliation for all the MCPTT groups contained in the list for the clients for which the <command-list> applies.

The recipient of the XML ignores any unknown element and any unknown attribute.

F.4.4 IANA registration template

Editor's note [CT1onMCPTT, C1ah-160012]: The MIME type application/ vnd.3gpp.mcptt-affiliation-command+xml as defined in this subclause is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcptt-affiliation-command+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.379 "Mission Critical Push To Talk (MCPTT) call control" version 13.0.0, available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical push to talk as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:
  i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG
  ii) Change controller: <MCC name>/<MCC email address>

F.5 XML schema for the floor request

F.5.1 General

This subclause defines XML schema and MIME type for application/vnd.3gpp.mcptt-floor-request+xml.

F.5.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="urn:3gpp:ns:mcpttFloorRequest:1.0"
xmlns:mcpttfloor="urn:3gpp:ns:mcpttFloorRequest:1.0">
    <!-- the root element -->
    <xs:element name="mcptt-floor-request" type="mcpttfloor:mcptt-floor-request-Type" minOccurs="1"
maxOccurs="2"/>
    <xs:complexType name="mcptt-floor-request-Type">
        <xs:sequence>
            <xs:element name="floor-type" type="xs:string"/>
            <xs:element name="ssrc" type="xs:unsignedLong"/>
            <xs:element name="floor-priority" type="xs:unsignedByte"/>
            <xs:element name="user-id" type="xs:anyURI"/>
            <xs:element name="track-info" type="mcpttfloor:track-info-Type"/>
            <xs:element name="floor-indicator" type="xs:unsignedLong"/>
            <xs:element name="anyExt" type="mcpttfloor:anyExtType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="anyExtType">
        <xs:sequence>
            <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="track-info-Type">
        <xs:sequence>
            <xs:element name="queueing-capability" type="xs:byte"/>
            <xs:element name="participant-type" type="xs:string"/>
            <xs:element name="floor-participant-reference" type="xs:unsignedLong" minOccurs="1"
maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttfloor:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
</xs:schema>
```

F.5.3 Semantic

This subclause describes the elements of the floor request XML Schema.

<floor-type> Contains information about which floor the current speaker was using. The value "general is selected when the current speaker has permission to speak in on the general floor as specified in 3GPP TS 24.380 [5] subclause 6.3.4. The value "dual" is selected when the current speaker has permission to speak in on the dual floor as specified in 3GPP TS 24.380 [5] subclause 6.3.6.

Table F.5.3-1 shows the ABNF of the <floor-type> element.

Table F.5.3-1: ABNF syntax of values of the <floor-type> element

```
floor-type-value = general-value / dual-value
general-value = %x67.65.6e.65.72.62.6c ; "general"
dual-value = %x64.75.61.6c ; "dual"
```

<ssrc>: Contains the SSRC of the floor participant. The content of the SSRC field shall be coded as specified in IETF RFC 3550 [10].

<floor-priority>: Contains the level of priority of the floor request. The <floor-priority> element is coded as specified in 3GPP TS 24.380 [5].

<user-id>: Contains the MCPTT ID of the MCPTT user requesting the permission to send media.

<track-info>: Contains the <queueing-capability> element, the <participant-type> element and the <floor-participant-reference>.

<floor-indicator>: Contains additional information. The <floor-indicator> element is coded as specified in 3GPP TS 24.380 [5].

<participant-type>: Contains the participant type assigned to the MCPTT user identified by the <user-id> element. The <participant-type> element is coded as specified in3GPP TS 24.380 [5].

NOTE: The reference to the floor participant is a value only understandable by the floor control server interface in the non-Controlling function of an MCPTT group.

<queueing-capability>: Contains the queueing capability of the MCPTT client. The <queueing-capability> element is coded as specified in 3GPP TS 24.380 [5].

The recipient of the XML ignores any unknown element and any unknown attribute.

F.5.4 IANA registration template

Editor's note [CT1#95-bis, CR 0100]: The MIME type "application/vnd.3gpp.mcptt-floor-request+xml" as defined in this subclause is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcptt-floor-request+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.379 "Mission Critical Push To Talk (MCPTT) call control" version 13.0.0, available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical push to talk as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>

- Author/Change controller:

  i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG

  ii) Change controller: <MCC name>/<MCC email address>

F.6 XML schema for integrity protection of MIME bodies

F.6.1 General

This subclause defines the XML schema and the MIME type vnd.3gpp.mcptt-signed+xml, for integrity protection of MIME bodies used in the present document.

F.6.2 XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:3gpp:ns:mcpttSignedDoc:1.0"
  xmlns:mcpttsigneddoc="urn:3gpp:ns:mcpttSignedDoc:1.0"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified"
  xmlns:xmldsig="http://www.w3.org/2000/09/xmldsig#">

  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>

  <xs:complexType name="signaturesType">
    <xs:sequence>
      <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="anyExt" type="mcpttsigneddoc:anyExtType" minOccurs="0"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <!-- root XML element when creating a signed XML document -->
  <xs:element name="signatures" type="mcpttsigneddoc:signaturesType"/>
  <xs:complexType name="anyExtType">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
```

F.6.3 Semantic

When integrity protection is turned on, the vnd.3gpp.mcptt-signed+xml MIME body is included when sending MIME bodies containing XML content in SIP requests and SIP responses.

The <signatures> element is the root element of the XML document.

NOTE 1: The subelements of the <signatures> element are validated by the <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <signatures> element

An instance of the <signatures> element contains one or more instances of the <xmldsig:Signature> element from the http://www.w3.org/2000/09/xmldsig# namespace. The <xmldsig:Signature> element validates against the <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> element.

Each <xmldsig:Signature> element contains the following child elements:

1) a <xmldsig:SignatureValue> element is included with a signature value;

2) a <xmldsig:SignedInfo> element can be included and can contain the following child elements:

a) a <xmldsig:CanonicalizationMethod> element can be included with an "Algorithm" attribute containing an appropriate canonicalisation method to be applied to the signed information;

b) a <xmldsig:SignatureMethod> element can be included with an "Algorithm" attribute containing an appropriate algorithm for the signature; and

NOTE 2: For signatures, it is assumed that HMAC-SHA256 is supported by the sender and the receiver.

c) a <xmldsig:Reference> element can be included and can contain the following child elements:

i) a "URI" attribute can be included with a "cid-URL" referring to an XML MIME body containing a Content-ID set to the "cid-URL"

ii) a <xmldsig:DigestMethod> element can be included referring to an appropriate method for hashing the content; and

NOTE 3: For hashing of the content, it is assumed that SHA-256 is supported by the sender and the receiver.

iii) a <xmldsig:DigestValue> element can be included containing the hashed content; and

3) a <xmldsig:KeyInfo> element can be included with a <xmldsig:KeyName> element containing the base 64 encoded XPK-ID.

NOTE 4: When the optional attributes and elements are not included within the <xmldsig:Signature> element, the information they contain is known to sender and the receiver by other means.

F.6.4 IANA registration template

Editor's note [CT1#95, C1-154478]: The MIME type application/vnd.3gpp.mcptt-signed+xml as defined in this subclause is to be registered in the IANA registry for Application Media Types based upon the following template. The registration is to be started when work on the MCPTT-CT WID completes.

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.mcptt-signed+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in section 9.1 of IETF RFC 7303.

Encoding considerations:

binary.

Security considerations:

Same as general security considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. In addition, this media type provides a format for exchanging information in SIP, so the security considerations from IETF RFC 3261 apply.

The information transported in this media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

This media type does not include provisions for directives that institute actions on a recipient's files or other resources.

This media type does not include provisions for directives that institute actions that, while not directly harmful to the recipient, may result in disclosure of information that either facilitates a subsequent attack or else violates a recipient's privacy in any way.

This media type does not employ compression.

Interoperability considerations:

Same as general interoperability considerations for application/xml media type as specified in section 9.1 of IETF RFC 7303. Any unknown XML elements and any unknown XML attributes are to be ignored by recipient of the MIME body.

Published specification:

3GPP TS 24.379 "Mission Critical Push To Talk (MCPTT) call control" version 13.1.0, available via http://www.3gpp.org/specs/numbering.htm.

Applications which use this media type:

Applications supporting the mission critical push to talk as described in the published specification.

Fragment identifier considerations:

The handling in section 5 of IETF RFC 7303 applies.

Restrictions on usage:

None

Provisional registration? (standards tree only):

N/A

Additional information:

1. Deprecated alias names for this type: none
2. Magic number(s): none
3. File extension(s): none
4. Macintosh File Type Code(s): none
5. Object Identifier(s) or OID(s): none

Intended usage:

Common

Person to contact for further information:

- Name: <MCC name>
- Email: <MCC email address>
- Author/Change controller:

  i) Author: 3GPP CT1 Working Group/3GPP_TSG_CT_WG1@LIST.ETSI.ORG

  ii) Change controller: <MCC name>/<MCC email address>

Annex G (informative): States managed by the MCPTT client and MCPTT server

G.1 MCPTT emergency state

The MCPTT emergency state is managed by the MCPTT client and MCPTT user. High-level characteristics of this state are captured in table G-1.1.

Table G.1-1: MCPTT emergency state

MCPTT emergency state	State-setting events	State-clearing events	Comments
Values: "set": MCPTT user is in a life-threatening situation "clear": MCPTT user is not in a life-threatening situation **Managed by:** MCPTT client and MCPTT user	MCPTT emergency alert initiated MCPTT emergency group call initiated MCPTT emergency private call initiated	MCPTT emergency alert cancelled (by initiator) MCPTT emergency alert cancelled (by authorised-user) MCPTT emergency call cancelled by initiator (if there is no outstanding MCPTT emergency alert) MCPTT user manually clears the state	While the MCPTT client is in the MCPTT emergency state, all group calls it makes will be MCPTT emergency group calls, providing the group is authorised for MCPTT emergency group calls. While in an emergency group call while in the MCPTT emergency state, the MCPTT user is an "emergency talker" and will have pre-emptive priority over non-emergency talkers in the emergency group call.

G.2 In-progress emergency group state

This state is described in both 3GPP TS 22.179 [2] and 3GPP TS 23.379 [3]. It is managed by the controlling MCPTT function. High-level characteristics of this state are captured in table G.2-1.

Table G.2-1: in-progress emergency group state

In-progress emergency group state values	State-entering events	Comments
"true"	acceptance by the controlling MCPTT function of an MCPTT emergency group call request (as per subclause 10.6.2.6.1.1 of 3GPP TS 23.379 [3]).	
"false"	initial state prior to any call activity acceptance by the controlling MCPTT function of an MCPTT emergency group cancel request (as per subclause 10.6.2.6.1.3 of 3GPP TS 23.379 [3]).	

G.3 MCPTT emergency group state

The MCPTT emergency group state is the MCPTT client's perspective of the in-progress emergency group state which is managed by the controlling MCPTT function. The MCPTT emergency group (MEG) state is managed by the MCPTT client to enable the requesting of MCPTT emergency-level priority as early as possible in the origination of an MCPTT emergency group call. High-level characteristics of this state are captured in table G.3-1.

Table G.3-1: MCPTT emergency group state

MCPTT emergency group state values	State-entering events	Comments
MEG 1: no-emergency	initial state prior to any call activity Emergency group call cancel request received on behalf of another user from the MCPTT server Emergency group call cancel response (success) in response to initiator's request	
MEG 2: in-progress	Emergency group call response received (confirm) to initiator's emergency group call request Emergency group call request received (on behalf of another user)	In this state, all participants in calls on this group will receive emergency level priority whether or not they are in the MCPTT emergency state themselves.
MEG 3: cancel-pending	Emergency group call cancel request sent by initiator	The controlling MCPTT server may not grant the cancel request for various reasons, e.g., other users in an MCPTT emergency state remain in the call.
MEG 4: confirm-pending	Emergency group call request sent by initiator	The controlling MCPTT server may not grant the call request for various reasons, e.g., the MCPTT group is not configured as being emergency-capable so it can't be assumed that the group will enter the in-progress state.

G.4 MCPTT emergency group call state

Table G.4-1 provides the semantics of the MCPTT emergency group call (MEGC) state values. This internal state of the MCPTT client and is managed by the MCPTT client. These states aid in the managing of the information elements of MCPTT emergency group calls and MCPTT emergency alerts and their cancellations.

Table G.4-1: MCPTT emergency group call state

MCPTT emergency group call state values	Semantics	Comments
MEGC 1: emergency-gc-capable	MCPTT client emergency-capable client is not currently in an MCPTT emergency group call that it has originated, nor is it in the process of initiating one.	**MCPTT emergency state:** may or may not be set in this state, depending upon the MCPTT client's MEA state
MEGC 2: emergency-call-requested	MCPTT client has initiated an MCPTT emergency group call request.	**MCPTT emergency state:** is set
MEGC 3: emergency-call-granted	MCPTT client has received an MCPTT emergency group call grant.	If the MCPTT user initiates a call while the MCPTT emergency state is still set, that call will be an MCPTT emergency group call, assuming that group is authorised for the client to initiate emergency group calls on. **MCPTT emergency state:** is set

G.5 MCPTT emergency alert state

Table G.5-1provides the semantics of the MCPTT emergency alert (MEA) state values. This is an internal state of the MCPTT client and is managed by the MCPTT client. These states aid in the managing of the information elements of MCPTT emergency group calls and MCPTT emergency alerts and their cancellations.

Table G.5-1: MCPTT emergency alert state

MCPTT emergency alert state values	State-entering events	Comments
MEA 1: no-alert	initial state emergency alert cancelled emergency alert request denied	emergency alerts can be cancelled in several ways: MCPTT emergency alert cancel request with <alert-ind> set to "false" (by initiator) MCPTT emergency alert cancel request with <alert-ind> set to "false" (by authorised user) MCPTT emergency group call cancel request with <alert-ind> set to "false" **MCPTT emergency state:** may be set or clear, depending on MCPTT emergency call status
MEA 2: emergency-alert-confirm-pending	emergency alert request sent	emergency alerts can be requested in several ways: MCPTT emergency alert request with <alert-ind> set to "true" MCPTT emergency group call request with <alert-ind> set to "true" **MCPTT emergency state:** is set
MEA 3: emergency-alert - initiated	emergency alert response (success) received	**MCPTT emergency state:** is set
MEA 4: emergency-alert-cancel-pending	emergency alert cancellation request sent by alert originator	**MCPTT emergency state:** is clear

G.6 In-progress imminent peril group state

This state is described in both 3GPP TS 22.179 [2] and 3GPP TS 23.379 [3]. It is managed by the controlling MCPTT function. High-level characteristics of this state are captured in table G.6-1.

Table G.6-1: in-progress imminent peril group state

In-progress imminent peril group state values	State-entering events	Comments
"true"	acceptance by the controlling MCPTT function of an MCPTT imminent peril group call request (as per subclause 10.6.2.6.2.1 and subclause 10.6.2.6.2.2 of 3GPP TS 23.379 [3]).	
"false"	initial state prior to any call activity acceptance by the controlling MCPTT function of an MCPTT imminent peril group cancel request (as per subclause 10.6.2.6.2.3 of 3GPP TS 23.379 [3]).	

G.7 MCPTT imminent peril group state

The MCPTT imminent peril group state is the MCPTT client's perspective of the in-progress imminent peril group state which is managed by the controlling MCPTT function. The MCPTT imminent peril group (MIG) state is managed by the MCPTT client to enable the requesting of MCPTT imminent peril-level priority as early as possible in the origination of an MCPTT imminent peril group call. High-level characteristics of this state are captured in table G.7-1.

Table G.7-1: MCPTT imminent peril group state

MCPTT imminent peril group state values	State-entering events	Comments
MIG 1: no-imminent peril	initial state prior to any call activity Imminent peril group call cancel request received on behalf of another user from the MCPTT server Imminent peril group call cancel response (success) in response to initiator's request	
MIG 2: in-progress	Imminent peril group call response received (confirm) to initiator's imminent peril group call request Imminent peril group call request received (on behalf of another user)	In this state, all participants in calls on this group will receive imminent peril level priority whether or not they initiated an MCPTT imminent peril group call themselves.
MIG 3: cancel-pending	Imminent peril group call cancel request sent by initiator	The controlling MCPTT server may not grant the cancel request for various reasons, e.g., other users in an MCPTT imminent peril state remain in the call.
MIG 4: confirm-pending	Imminent peril group call request sent by initiator	The controlling MCPTT server may not grant the call request for various reasons, e.g., the MCPTT group is not configured as being imminent peril-capable so it can't be assumed that the group will enter the in-progress state.

G.8 MCPTT imminent peril group call state

Table G.8-1 provides the semantics of the MCPTT imminent peril group call (MIGC) state values. This internal state of the MCPTT client and is managed by the MCPTT client. These states aid in the managing of the information elements of MCPTT imminent peril group calls and their cancellations.

Table G.8-1: MCPTT imminent peril group call state

MCPTT imminent peril group call state values	Semantics	Comments
MIGC 1: imminent peril-gc-capable	MCPTT client imminent peril-capable client is not currently in an MCPTT imminent peril group call that it has originated, nor is it in the process of initiating one.	In this state, the MCPTT imminent peril group state will be set to either "MIG 1: no-imminent-peril" or "MIG 2 in-progress" state.
MIGC 2: imminent peril-call-requested	MCPTT client has initiated an MCPTT imminent peril group call request.	In this state, the MCPTT imminent peril group state will be set to "MIG 4: confirm-pending" if not already in the "MIG 2 in-progress" state.
MIGC 3: imminent peril-call-granted	MCPTT client has received an MCPTT imminent peril group call grant.	In this state, the MCPTT imminent peril group state will be set to "MIG2 in-progress".

G.9 In-progress emergency private call state

This state is managed by the controlling MCPTT function. All private calls originated between an initiator and the target MCPTT user when they are in an in-progress emergency private call state are MCPTT emergency private calls until this state is cancelled, whether or not the originator of the private call is in an MCPTT emergency state.

Table G.9-1: in-progress emergency private call state

In-progress emergency private call state values	State-entering events	Comments
"true"	acceptance by the controlling MCPTT function of an MCPTT emergency private call request (as per subclause 10.7.2.4.1 of 3GPP TS 23.379 [3]).	The in-progress emergency private call state applies to the call and the two MCPTT users in the call.
"false"	initial state prior to any private call activity acceptance by the controlling MCPTT function of the cancellation of an MCPTT emergency private call (as per subclause 10.7.2.4.1 of 3GPP TS 23.379 [3]).	

G.10 MCPTT emergency private priority state

The MCPTT emergency private priority state is the MCPTT client's perspective of the in-progress emergency private call state which is managed by the controlling MCPTT function. The MCPTT emergency private priority (MEPP) state is managed by the MCPTT client to enable the requesting of MCPTT emergency-level priority as early as possible in the origination of an MCPTT emergency private call. High-level characteristics of this state are captured in table G.10-1.

Table G.10-1: MCPTT emergency private priority state

MCPTT emergency private priority state values	State-entering events	Comments
MEPP 1: no-emergency	initial state prior to any call activity Emergency private call cancel request received on behalf of another user from the MCPTT server Emergency private call cancel response (success) in response to initiator's request	
MEPP 2: in-progress	Emergency private call response received (confirm) to initiator's emergency private call request Emergency private call request received (on behalf of another user)	In this state, both participants in calls to each other will request emergency level priority whether or not they are in the MCPTT emergency state themselves.
MEPP 3: cancel-pending	Emergency private call cancel request sent by initiator	The controlling MCPTT server may not grant the cancel request for various reasons, e.g., the other user in the call is in an MCPTT emergency state.
MEPP 4: confirm-pending	Emergency private call request sent by initiator	The controlling MCPTT server may not grant the call request for various reasons, e.g., the MCPTT user is not configured as being authorised to originate an emergency private call so it can't be assumed that the call (originator and target users) will enter the in-progress state.

G.11 MCPTT emergency private call state

Table G.11-1 provides the semantics of the MCPTT emergency private call (MEPC) state values. This is an internal state of the MCPTT client and is managed by the MCPTT client. This state aids in the managing of the information elements of MCPTT emergency private calls and MCPTT emergency alerts and their cancellations.

Table G.11-1: MCPTT emergency private call state

MCPTT emergency private call state values	Semantics	Comments
MEPC 1: emergency-pc-capable	MCPTT client emergency-capable client is not currently in an MCPTT emergency private call that it has originated, nor is it in the process of initiating one.	**MCPTT emergency state:** may or may not be set in this state, depending upon the MCPTT client's MPEA state and the emergency states related to MCPTT emergency group calls.
MEPC 2: emergency-pc-requested	MCPTT client has initiated an MCPTT emergency private call request.	**MCPTT emergency state:** is set
MEPC 3: emergency-pc-granted	MCPTT client has received an MCPTT emergency private call grant.	If the MCPTT user initiates a call while the MCPTT emergency state is still set, that call will be an MCPTT emergency private call, assuming that the initiating MCPTT user is authorised to initiate an MCPTT emergency private call to the targeted MCPTT user. **MCPTT emergency state:** is set

G.12 MCPTT private emergency alert state

Table G.5-1provides the semantics of the MCPTT private emergency alert (MPEA) state values. This is an internal state of the MCPTT client and is managed by the MCPTT client. These states aid in the managing of the information elements of MCPTT emergency private calls and MCPTT emergency alerts and their cancellations. MCPTT private emergency alerts are targeted to an MCPTT user.

Table G.12-1: MCPTT private emergency alert state

MCPTT emergency alert state values	State-entering events	Comments
MPEA 1: no-alert	initial state emergency alert cancelled emergency alert request denied	emergency alerts targeted to an MCPTT user can be cancelled in several ways: MCPTT emergency private call cancel request with <alert-ind> set to "false" timeout of private call inactivity timer end of call (if system policy) **MCPTT emergency state:** may be set or clear, depending on MCPTT emergency call status
MPEA 2: emergency-alert-confirm-pending	emergency alert request sent	emergency alerts can be requested as an optional part of a MCPTT client's request to initiate an MCPTT emergency private call, in which case the request has an <alert-ind> element set to "true". **MCPTT emergency state:** is set
MPEA 3: emergency-alert - initiated	emergency alert response (success) received	**MCPTT emergency state:** is set
MPEA 4: emergency-alert-cancel-pending	emergency alert cancellation request sent by alert originator	**MCPTT emergency state:** is clear

G.13 Private call call-back state information

Table G.13-1 provides the semantics of the private call call-back state values that are managed by an MCPTT client that initiates a private call call-back request or a private call call-back cancel request. Such a client is known as a requesting MCPTT client.

Table G.13-2 provides the semantics of the private call call-back state values that are managed by an MCPTT client that receives a private call call-back request or a private call call-back cancel request. Such a client is known as a target MCPTT client.

Table G.13-1: MCPTT private call call-back requesting client states

MCPTT private call call-back requesting client states	State-entering events	Comments
PCCB-I1: no-call-back	Moving from "PCCB-I4: cancel-pending" when the requesting MCPTT client receives a private call call-back cancel response from the target MCPTT client Moving from "PCCB-I3: confirmed" when the requesting MCPTT client sends a response to a private call set-up establishment request from the target MCPTT client.	The information stored on the requesting MCPTT client for the target MCPTT user is deleted.
PCCB-I2: confirm-pending	Moving from "PCCB-I1: no call-back" when the rqeuesting MCPTT client has sent a private call call-back request and is awaiting the response back from the target MCPTT client.	Temporary state of the UE, while the UE awaits the response to the call back request from the target MCPTT client.
PCCB-I3: confirmed	Moving from "PCCB-I2: confirm-pending" when the requesting MCPTT client receives the private call call-back response from the target MCPTT client	The client stores the MCPTT ID of the remote client and the requesting client state. In this state, the client is expecting to receive a private call from the remote client.
PCCB-I4: cancel-pending	Moving from "PCCB-I3: confirmed" when the requesting MCPTT client has initiated a private call cancel request towards the target MCPTT client	Temporary state while the UE awaits the cancel response from the target MCPTT client.

Table G.13-2: MCPTT private call call-back target client states

MCPTT private call call-back target client states	State-entering events	Comments
PCCB-R1: no-call-back	Moving from "PCCB-R2: private-call-call-back-pending" upon initiating a private call to the requesting MCPTT client, and receiving the SIP 200 (OK) to the private call request.	The information stored on the target MCPTT client for the requesting MCPTT user is deleted.
PCCB-R2: private-call-pending	Moving from "PCCB-R1: no call-back" when the target MCPTT client has received a private-call call-back request from the requesting MCPTT client, and has confirmed this by sending a response to this client.	The client stores the MCPTT ID, target client state, urgency and time of request.

Annex H (informative): On-network routing considerations

H.1 General

The following subclauses summarise the identities placed into SIP headers and SIP bodies during session establishment.

H.2 Group Call

Table H.2-1 describes the contents of the SIP headers and SIP bodies inserted by MCPTT clients and MCPTT servers involved in a group call.

Table H.2-1: Routing considerations for group call

Interface	Content of SIP headers	Content of "mcptt-info" MIME body	Notes
originating MCPTT client to originating participating MCPTT function (O-PF).	Request-URI contains PSI of O-PF. P-Preferred-Identity may contain IMPU of originating user.	"mcptt-request-uri" contains the group identity.	PSI of O-PF configured for each client. MCPTT-id of each client is never sent in session initiation.
O-PF to controlling MCPTT function (CF).	Request-URI contains PSI of CF. P-Asserted-Identity contains IMPU of originating user.	"mcptt-request-uri" contains the group identity. "mcptt-calling-user-id" contains MCPTT ID of originating user.	CF finds the MCPTT ID of the originating user from the stored IMPU-MCPTT ID binding and locates the PSI of the controller that serves the group identity. O-PF contains configuration of the PSIs of the CFs.
CF to terminating participating MCPTT function (T-PF).	Request-URI contains the address of the T-PF. P-Asserted-Identity contains the address of the CF.	"mcptt-request-uri" contains the MCPTT ID of the terminating user. "mcptt-calling-user-id" contains MCPTT ID of originating user. "mcptt-calling-group-id" contains the group identity.	For each client in the group, CF maps the MCPTT-ID of the terminator to the address of the T-PF. If the terminator is in another domain, the CF can map the MCPTT ID of the terminator to a PSI identifying a interrogating function in the partner network that is able to find the T-PF using the MCPTT ID.
CF to non-controlling MCPTT function of an MCPTT group (NCF).	Request-URI contains the PSI of the NCF. P-Asserted-Identity contains the PSI of the CF.	"mcptt-request-uri" contains the group identity. "mcptt-calling-user-id" contains MCPTT ID of originating user.	-
T-PF to terminating MCPTT client.	Request-URI contains the IMPU of the terminating user. P-Asserted-Identity contains the address of the CF.	"mcptt-request-uri" contains the MCPTT ID of the terminating user. "mcptt-calling-user-id" contains MCPTT ID of originating user. "mcptt-calling-group-id" contains the group identity.	T-PF finds the IMPU of the terminating user from the stored IMPU-MCPTT ID binding at the time of registration.
terminating MCPTT client to T-PF (response).	as in TS 24.229.	"mcptt-called-party-id" contains contacted client's MCPTT ID.	-
T-PF to NCF (response)	as in TS 24.229	"mcptt-called-party-id" contains contacted client's MCPTT ID.	-
T-PF to CF (response).	as in TS 24.229.	"mcptt-called-user" contains contacted client's MCPTT ID.	-
NCF to CF (response)	as in TS 24.229.	-	In the case of trusted mutual aid, the NCF returns the identities of the group in a "resource-lists" MIME body.
CF to O-PF (response)	as in TS 24.229.	-	-
O-PF to originating MCPTT client (response)	as in TS 24.229.	-	-

H.3 Private Call

Table H.3-1 describes the contents of the SIP headers and SIP bodies inserted by MCPTT clients and MCPTT servers involved in a private call.

Table H.3-1: Routing considerations for private call

Interface	Content of SIP headers	Content of SIP bodies (body in brackets)	Notes
originating MCPTT client to originating participating MCPTT function (O-PF)	Request-URI contains the PSI for the private call service. P-Preferred-Identity may contain IMPU of originating user	MCPTT ID of called user (resource-lists)	PSI for private call is configured on the client.
O-PF to controlling MCPTT function (CF)	Request-URI contains the PSI for the private call service. P-Asserted-Identity contains IMPU of originating user.	MCPTT ID of called user (resource-lists) MCPTT ID of calling user contained in "mcptt-calling-user-id" (mcptt-info)	-
CF to terminating participating MCPTT function (T-PF)	Request-URI contains the address of the T-PF. P-Asserted-Identity contains IMPU of originating user.	MCPTT ID of calling user contained in "mcptt-calling-user-id" (mcptt-info). MCPTT ID of called user contained in "mcptt-called-party-id" (mcptt-info).	If the terminator is in another domain, the CF can map the MCPTT ID of the terminator to a PSI identifying an interrogating function in the partner network that is able to find the T-PF using the MCPTT ID.
T-PF to terminating MCPTT client	Request-URI contains the IMPU of the terminating user. P-Asserted-Identity contains IMPU of originating user.	MCPTT ID of calling user contained in "mcptt-calling-user-id" (mcptt-info). MCPTT ID of called user contained in "mcptt-called-party-id" (mcptt-info).	-
terminating MCPTT client to T-PF (response)	as in TS 24.229	"mcptt-called-party-id" contains contacted client's MCPTT ID (mcptt-info).	-
T-PF to CF (response)	as in TS 24.229	"mcptt-called-user" contains contacted client's MCPTT ID (mcptt-info).	-
CF to O-PF (response)	as in TS 24.229	"mcptt-called-party-id" contains contacted client's MCPTT ID (mcptt-info).	-
O-PF to originating MCPTT client (response)	as in TS 24.229	"mcptt-called-party-id" contains contacted client's MCPTT ID (mcptt-info).	-

Annex I (normative): MCPTT Off-Network Protocol (MONP) message coding rules

I.1 General

The following subclauses describe the message coding rules for the MCPTT Off-Network Protocol (MONP).

I.2 MONP messages

I.2.1 Components of a MONP message

A standard MONP message consists of an imperative part, itself composed of a header and the rest of imperative part, followed by a non-imperative part. Both the non-header part of the imperative part and the non-imperative part are composed of successive parts referred as standard information elements.

I.2.2 Format of standard information elements

A standard IE may have the following parts, in that order:

- an information element identifier (IEI);
- a length indicator (LI);
- a value part.

A standard IE has one of the formats shown in table I.2.2-1:

Table I.2.2-1: Formats of information elements

Format	Meaning	IEI present	LI present	Value part present
T	Type only	yes	no	no
V	Value only	no	no	yes
TV	Type and Value	yes	no	yes
LV	Length and Value	no	yes	yes
TLV	Type, Length and Value	yes	yes	yes
LV-E	Length and Value	no	yes	yes
TLV-E	Type, Length and Value	yes	yes	yes

Some IEs may appear in the structure, but not in all instances of messages. An IE is then said to be present or not present in the message instance. If an IE is not present in a message instance, none of the three parts is present. Otherwise, parts must be present according to the IE format.

In the message structure, an IE that is allowed not to be present in all message instances is said not to be mandatory. Other IEs are said to be mandatory.

I.2.2.1 Information element type and value part

Every standard IE has an information element type which determines the values possible for the value part of the IE, and the basic meaning of the information. The information element type describes only the value part. Standard IEs of the same information element type may appear with different formats. The format used for a given standard IE in a given message is specified within the description of the message.

The value part of a standard IE either consists of a half octet or one or more octets; the value part of a standard IE with format LV or TLV consists of an integral number of octets, between 0 and 255 inclusive; it then may be empty, i.e., consist of zero octets; if it consists of a half octet and has format TV, its IEI consists of a half octet, too. For LV-E and TLV-E, the value part of a standard IE consists of an integral number of octets, between 0 and 65535 inclusive. The value part of a standard IE may be further structured into parts, called fields.

I.2.2.2 Length indicator

For LV or TLV, the length indicator (LI) of a standard IE consists of one octet. For LV-E and TLV-E, the LI of a standard IE consists of two octets where bit 8 of octet n contains the most significant bit and bit 1 of octet n+1 contains the least significant bit (refer to figure I.2.2.4-9 in subclause I.2.2.4 for the relative ordering of the 2 octets). The LI contains the binary encoding of the number of octets of the IE value part. The LI of a standard IE with empty value part indicates 0 octets. Standard IE of an information element type such that the possible values may have different values must be formatted with a length field, i.e., LV, TLV, LV-E or TLV-E.

I.2.2.3 Information element identifier

When present, the IEI of a standard IE consists of a half octet or one octet. A standard IE with IEI consisting of a half octet has format TV, and its value part consists of a half octet. The value of the IEI depends on the standard IE, not on its information element type. The IEI, if any, of a given standard IE in a given message is specified within the description of the message. In some protocol specifications, default IEI values can be indicated. They are to be used if not indicated in the message specification. Non mandatory standard IE in a given message, i.e., IE which may be not be present (formally, for which the null string is acceptable in the message), must be formatted with an IEI, i.e., with format T, TV, TLV or TLV-E.

I.2.2.4 Categories of IEs; order of occurrence of IEI, LI, and value part

The following categories of standard information elements are defined:

- information elements of format V or TV with value part consisting of 1/2 octet (type 1);
- information elements of format T with value part consisting of 0 octets (type 2);
- information elements of format V or TV with value part that has fixed length of at least one octet (type 3);
- information elements of format LV or TLV with value part consisting of zero, one or more octets (type 4)
- information elements of format LV-E or TLV-E with value part consisting of zero, one or more octets and a maximum of 65535 octets (type 6).

NOTE: The "types" and "formats" used for MONP match those defined in 3GPP TS 24.007 [56];

Type 1 standard information elements of format V provide the value in bit positions 8, 7, 6, 5 of an octet (see figure I.2.2.4-1) or bits 4, 3, 2, 1 of an octet (see figure I.2.2.4-2).

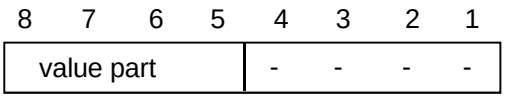

Figure I.2.2.4-1: Type 1 IE of format V

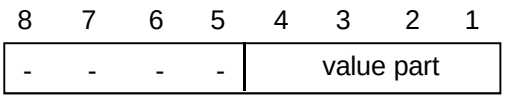

Figure I.2.2.4-2: Type 1 IE of format V

Type 1 standard information elements of format TV have an IEI of a half octet length; they provide the IEI in bit positions 8, 7, 6, 5 of an octet and the value part in bit positions 4, 3, 2, 1 of the same octet, see figure I.2.2.4-3.

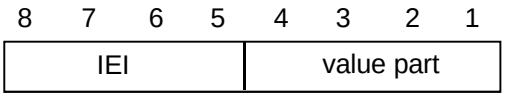

Figure I.2.2.4-3: Type 1 IE of format TV

A type 2 standard IE has format T; its IEI consists of one octet, its value part is empty, see figure I.2.2.3-4.

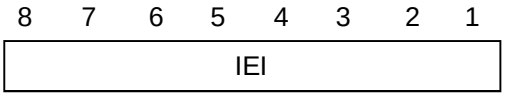

Figure I.2.2.4-4: Type 2 IE

A type 3 standard information element has format V or TV; if it has format TV, its IEI consists of one octet and proceeds the value part in the IE. The value part consists of at least one octet. See figure I.2.2.4-5 and figure I.2.2.4-6.

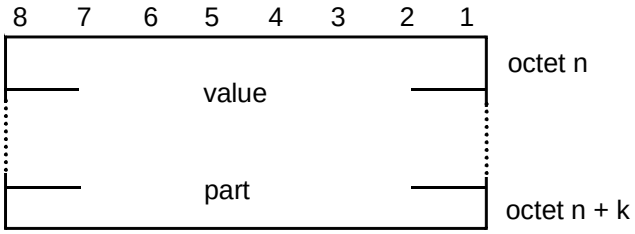

Figure I.2.2.4-5: Type 3 IE of format V (k = 0, 1, 2, ...)

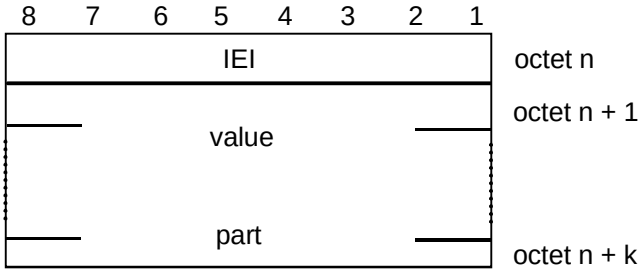

Figure I.2.2.4-6: Type 3 IE of format TV (k = 1, 2, ...)

A type 4 standard information element has format LV or TLV. Its LI precedes the value part, which consists of zero, one, or more octets; if present, its IEI has one octet length and precedes the LI. See figure I.2.2.4-7 and figure I.2.2.4-8.

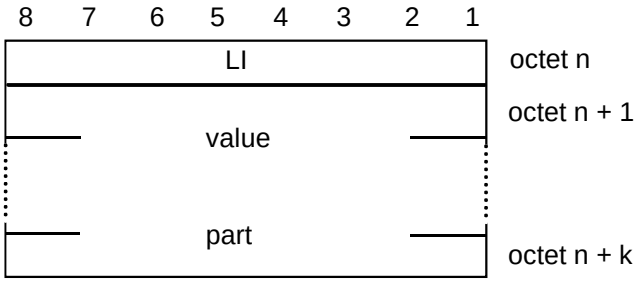

Figure I.2.2.4-7: Type 4 IE of format LV (k = 0, 1, 2, ...)

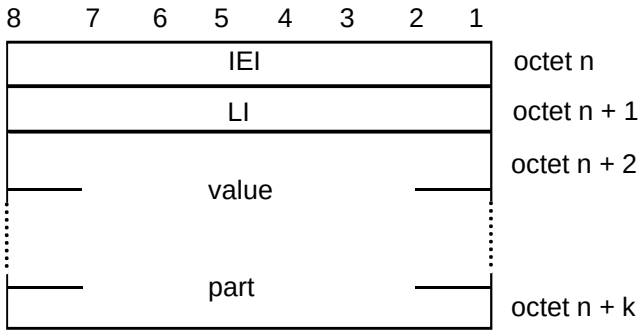

Figure I.2.2.4-8: Type 4 IE of format TLV (k = 1, 2, ...)

A type 6 standard information element has format TLV-E. The IEI has one octet length and precedes the LI of 2 octets and the value part which consists of zero, one or up to 65535 octets. See figure I.2.2.4-9 and figure I.2.2.4-10.

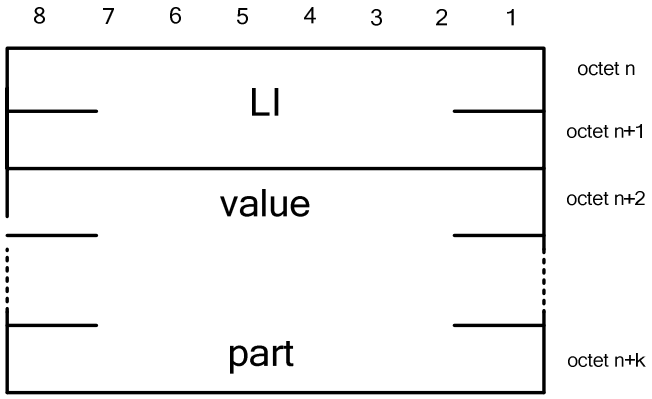

Figure I.2.2.4-9: Type 6 IE of format LV-E (k = 1, 2, ...)

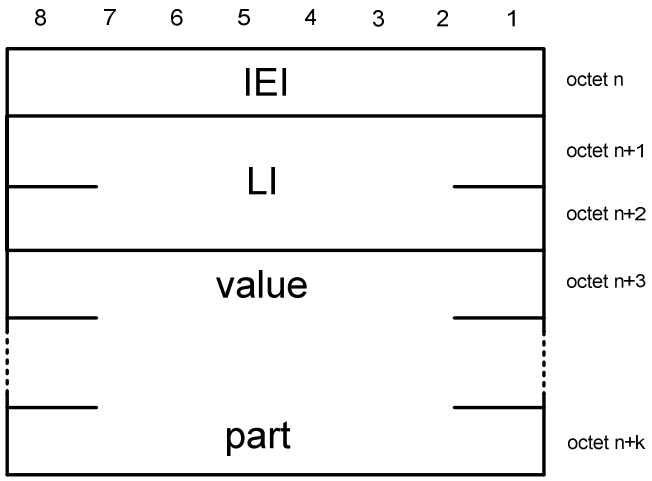

Figure I.2.2.4-10: Type 6 IE of format TLV-E (k = 1, 2, ...)

I.2.2.5 Method for IE structure

Standard IEs can be further structured in parts called fields and represented in a tabular form.

The IE is presented in its maximum format, i.e., T, TV, TLV or TLV-E, in a picture representing the bits in a table, each line representing an octet. Bits appear in the occidental order, i.e., from left of the page to right of the page, and from top of the page to bottom of the page.

Boxes so delimited contains typically the field name, possibly an indication of which bits in the field are in the box, and possibly a value (e.g., for spare bits).

A specific method can be used in the IE description to describe a branching structure, i.e., a structure variable according to the value of particular fields in the IE. This design is unusual outside type 4 and type 6 IEs, and as, a design rule, should be used only in type 4 and type 6 IEs.

a) The octet number of an octet within the IE is defined typically in the table. It consists of a positive integer, possibly of an additional letter, and possibly of an additional asterisk, see clause f). The positive integer identifies one octet or a group of octets.

b) Each octet group is a self-contained entity. The internal structure of an octet group may be defined in alternative ways.

c) An octet group is formed by using some extension mechanism. The preferred extension mechanism is to extend an octet (N) through the next octet(s) (Na, Nb, etc.) by using bit 8 in each octet as an extension bit.

   - The bit value "0" indicates that the octet group continues through to the next octet. The bit value "1" indicates that this octet is the last octet of the group. If one octet (Nb) is present, the preceding octets (N and Na) shall also be present.

   - In the format descriptions of the individual information elements, bit 8 is marked "0/1 ext" if another octet follows. Bit 8 is marked "1 ext" if this is the last octet in the extension domain.

   - Additional octets may be defined in later versions of the protocols ("1 ext" changed to "0/1 ext") and equipments shall be prepared to receive such additional octets; the contents of these octets shall be ignored. However the length indicated in the formal description of the messages and of the individual information elements only takes into account this version of the protocols.

d) In addition to the extension mechanism defined above, an octet (N) may be extended through the next octet(s) (N+1, N+2 etc.) by indications in bits 7-1 (of octet N).

e) The mechanisms in c) and d) may be combined.

f) Optional octets are marked with asterisks (*). As a design rule, the presence or absence of an optional octet should be determinable from information in the IE and preceding the optional octet. Care should be taken not to introduce ambiguities with optional octets.

g) At the end of the IE, additional octets may be added in later versions of the protocols also without using the mechanisms defined in c) and d). Equipments shall be prepared to receive such additional octets; the contents of these octets shall be ignored. However the length indicated in the formal description of the messages and of the individual information elements only takes into account this version of the protocols.

I.2.2.6 Imperative part of a standard MONP message

I.2.2.6.0 General

The imperative part of a standard MONP message is composed of a header possibly followed by mandatory standard IEs having the format V, LV or LV-E.

The header consists of a message type information element as specified in subclause 15.2.1.

I.2.2.6.1 Standard information elements of the imperative part

The message type octet of a standard MONP message may be followed by mandatory standard IEs having the format V, LV or LV-E as specified in the message description in the relevant protocol specification.

As a design rule, octet boundaries must be respected. This implies that half-octet standard IEs (i.e., V formatted type 1 standard IEs) must appear by pair.

If message is received as a standard MONP message, and that is too short to contain the complete imperative part as specified in the relevant protocol specification, an imperative message part error is diagnosed. (The same error may be

diagnosed at detection of certain contents of the imperative part of a message; this is defined in the relevant protocol specification.) The treatment of an imperative message part error is defined in the relevant protocol specification.

I.2.2.7 Non-imperative part of a standard MONP message

The imperative part of a standard MONP message may be followed by the non-imperative part. The MONP protocol specification defines where the imperative part of a standard MONP message ends. The non-imperative part of a standard MONP message is composed of (zero, one, or several) standard IEs having the format T, TV, TLV or TLV-E. The receiver of a standard MONP message shall analyse the non-imperative part as a succession of standard IEs each containing an IEI, and shall be prepared for the non-imperative part of the message to contain standard IEs that are not specified in the relevant protocol specification.

An IEI may be known in a message or unknown in a message.

An IEI that is known in a message designates the IE type of the IE the first part of which the IEI is, as well as the use of the information. Which IE type it designates is specified in the relevant protocol specification. Within a message, different IEIs may designate the same IE type if that is defined in the relevant protocol specification.

Whether the second part of an IE with IEI known in a message is the length or not (in other words, whether the IEI is the first part of an IE formatted as TLV, TLV-E or not) is specified in the relevant protocol specification.

Unless otherwise specified in the protocol specification, the receiver shall assume that IE with unknown IEI are TV formatted type 1, T formatted type 2, TLV formatted type 4 or TLV-E formatted type 6 standard IEs. The IEI of unknown IEs together with, when applicable, the length indicator, enable the receiver to determine the total length of the IE, and then to skip unknown IEs. The receiver shall assume the following rule for IEs with unknown IEI:

> Bit 8 of the IEI octet is set to "1" indicates a TV formatted type 1 standard IE or a T formatted type 2 IEs. Hence, a 1 valued bit 8 indicates that the whole IE is one octet long.

Furthermore:

> Bit 8 of the IEI octet set to "0" and bits 7 to 4 set to "1" indicates a TLV-E formatted type 6 IE, i.e. the following two octets are length octets. Bit 8 of the IEI octet set to "0" and bit 7 to 4 set to any other bit combination indicates a TLV formatted type 4 IE, i.e. the following octet is a length octet.

As a design rule, it is recommended that IEIs of any TV formatted type 1, T formatted type 2, TLV formatted type 4 or TLV-E formatted type 6 IE follow the rule, even if assumed to be known by all potential receivers.

A message may contain two or more IEs with equal IEI. Two IEs with the same IEI in a same message must have the same format, and, when of type 3, the same length. More generally, care should be taken not to introduce ambiguities by using an IEI for two purposes. Ambiguities appear in particular when two IEs potentially immediately successive have the same IEI but different meanings and when both are non-mandatory. As a recommended design rule, messages should contain a single IE of a given IEI.

Each protocol specification may put specific rules for the order of IEs in the non-imperative part. An IE known in the message, but at a position non-compliant with these rules is said to be out of sequence. An out of sequence IE is decoded according to the format, and, when of type 3 the length, as defined in the message for its IEI.

I.2.2.8 Presence requirements of information elements

The relevant protocol specification may define three different presence requirements (M, C, or O) for a standard IE within a given standard MONP message:

- M ("Mandatory") means that the IE shall be included by the sending side, and that the receiver diagnoses a "missing mandatory IE" error when detecting that the IE is not present. An IE belonging to the imperative part of a message has presence requirement M. An IE belonging to the non-imperative part of a message may have presence requirement M;

- C ("Conditional") means:

  * that inclusion of the IE by the sender depends on conditions specified in the relevant protocol specification;

  * that there are conditions for the receiver to expect that the IE is present and/or conditions for the receiver to expect that the IE is not present in a received message of a given message type; these conditions depend only

on the content of the message itself, and not for instance on the state in which the message was received, or on the receiver characteristics; they are known as static conditions;

* that the receiver detecting that the IE is not present when sufficient static conditions are fulfilled for its presence, shall diagnose a "missing conditional IE" error;

* that the receiver detecting that the IE is present when sufficient static conditions are fulfilled for its non-presence, shall diagnose an "unexpected conditional IE" error.

- Only IEs belonging to the non-imperative part of a message may have presence requirement C;

- O ("Optional") means that the receiver shall never diagnose a "missing mandatory IE" error, a "missing conditional IE" error, or an "unexpected conditional IE" error because it detects that the IE is present or that the IE is not present. (There may however be conditions depending on the states, resources, etc. of the receiver to diagnose other errors.) Only IEs belonging to the non-imperative part of a message may have presence requirement O.

Unless otherwise specified the presence of an IE of unknown IEI or of an out of sequence IE shall not lead by itself to an error.

I.2.2.9 Description of standard MONP messages

This subclause describes a generic description method for MONP messages, the tabular description.

A MONP message is described by a table listing the header elements and the standard IEs in the message. For each element is given:

- if applicable the IEI, in hexadecimal representation (one digit followed by and hyphen for TV formatted type 1, and two digits for the other cases);

- the name of the IE (this is used in particular for the description of conditional presence rules);

- the type of the information element, with a reference of where the internal structure of the value part is specified;

- the format of the standard IE (T, V, TV, LV, TLV, LV-E or TLV-E); and

- the length, or the range of lengths, of the whole standard IE, including when applicable the T and L parts.

The list of elements is given in the table in the order they appear in the resulting bit string, with the exception of half-octet elements in the imperative part: half octets in a pair are inverted.

Annex J (informative): INFO packages defined in the present document

J.1 Info package for transfer of floor requests

J.1.1 Scope

This subclause contains the information required for the IANA registration of info package g.3gpp.mcptt-floor-request in accordance with IETF RFC 6086 [64].

J.1.2 g.3gpp.mcptt-floor-request info package

J.1.2.1 Overall description

When a temporary group call includes constituent MCPTT groups in partner systems where a MCPTT call is ongoing and if the floor is occupied by a participant with a permission to speak, the non-controlling MCPTT function of a MCPTT group needs to transfer information of the current speaker(s) to the controlling MCPTT function hosting the temporary group. The information is transferred in the form of a floor request.The controlling MCPTT function will then determine if the participant will be permitted to continue to speak or if the permission to speak is revoked.

J.1.2.2 Applicability

This package is used to transport a floor request from the non-controlling MCPTT function of an MCPTT group to the controlling MCPTT function hosting the temporary group.

J.1.2.3 Appropriateness of INFO Package Usage

A number of solutions were discussed for the transportation of the floor request to the controlling MCPTT function hosting the temporary MCPTT group. The solutions were:

1) Use of the session related methods (e.g. SIP 200 (OK) response to the SIP INVITE request).
2) Use of the SIP MESSAGE method.
3) Use of the SIP INFO method as described in IETF RFC 6086, by defining a new info package.

The result of the evaluation of the above solutions were:

1) To include such a large amount of data in a SIP 200 (OK) response to an SIP INVITE request could cause problems with the size of the SIP 200 (OK) response resulting in packet fragmentation.
2) The use of the SIP MESSAGE request would result in that the recommended value of size of the information transferred by the SIP MESSAGE request would be exceeded.
3) The use of SIP INFO request was found as the most appropriate solution since the SIP INFO request could be sent in the existing SIP session.

J.1.2.4 Info package name

g.3gpp.mcptt-floor-request

J.1.2.5 Info package parameters

None defined

J.1.2.6 SIP options tags

None defined

J.1.2.7 INFO message body parts

The MIME type of the message body carrying participant identities is application/vnd.3gpp.floor-request+xml. The application/vnd.3gpp.floor-request+xml MIME type is defined in 3GPP TS 24.379.

When associated with the g.3gpp.mcptt-floor-request info package, the Content-Disposition value of the message body carrying the floor request is "info-package".

J.1.2.8 Info package usage restrictions

None defined.

J.1.2.9 Rate of INFO Requests

Single INFO request generated after session set up.

J.1.2.10 Info package security considerations

The security is based on the generic security mechanism provided for the underlying SIP signalling. No additional security mechanism is defined.

J.1.2.11 Implementation details and examples

UAC generation of INFO requests: See 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification".

UAS processing of INFO requests: See 3GPP TS 24.379: ""Mission Critical Push To Talk (MCPTT) call control; Protocol specification"

EXAMPLE: A controlling MCPTT function hosting a temporary MCPTT group inviting a constituent MCPTT group hosted by a non-controlling MCPTT function of a MCPTT group in a partner system where an MCPTT call is ongoing with one or two of the participants granted to speak. Then the non-controlling MCPTT function of the an MCPTT group sends a SIP INFO request carrying a floor request in an application/vnd.3gpp.mcptt-floor-request+xml MIME body using the g.3gpp.mcptt-floor-request info package.

J.2 Info package for transfer of MCPTT information

J.2.1 Scope

This subclause contains the information required for the IANA registration of info package g.3gpp.mcptt-info in accordance with IETF RFC 6086 [64].

J.2.2 g.3gpp.mcptt-info info package

J.2.2.1 Overall description

The MCPTT client request for MCPTT emergency call origination can also optionally request the origination of an MCPTT emergency alert. Similarly, the MCPTT client request for MCPTT emergency call cancellation can also optionally request the cancellation of an MCPTT emergency alert. A mechanism to inform the MCPTT client that one of the requested actions has been rejected by the controlling MCPTT function is needed to both inform the MCPTT user

that one of their requested actions has been rejected and to keep the emergency and imminent peril related state machines maintained by the MCPTT client updated appropriately. Note that a SIP 200 OK has to be sent in the case where the MCPTT emergency call origination request or cancellation request is accepted by the controller to allow the MCPTT user to initiate the MCPTT emergency call and receive updated priority even if the accompanying MCPTT alert request is rejected.

An MCPTT client request for an MCPTT imminent peril call when the targeted MCPTT group is in an in-progress emergency state also needs special handling, as in this case, the call request will be accepted but the MCPTT client needs to be informed that the MCPTT user will be joined to an in-progress MCPTT emergency group call instead of the requested MCPTT imminent peril group call to keep the emergency and imminent peril related state machines maintained by the MCPTT client updated appropriately.

J.2.2.2 Applicability

This package is used to transport emergency call, imminent peril and emergency alert indications from the controlling function to the MCPTT client

J.2.2.3 Appropriateness of INFO Package Usage

A number of solutions were discussed for the transportation of the emergency call, imminent peril and emergency alert indications from the controlling function to the MCPTT client. The solutions were:

1) Use of the session related methods (e.g. SIP 200 (OK) response to the SIP INVITE request).

2) Use of the SIP MESSAGE method.

3) Use of the SIP INFO method as described in IETF RFC 6086, by defining a new info package.

The result of the evaluation of the above solutions were:

1) To include such a large amount of data in a SIP 200 (OK) response to an SIP INVITE request could cause problems with the size of the SIP 200 (OK) response resulting in packet fragmentation.

2) The use of the SIP MESSAGE request would result in that the recommended value of size of the information transferred by the SIP MESSAGE request would be exceeded.

3) The use of SIP INFO request was found as the most appropriate solution since the SIP INFO request could be sent in the existing SIP session.

J.2.2.4 Info package name

g.3gpp.mcptt-info

J.2.2.5 Info package parameters

None defined

J.2.2.6 SIP options tags

None defined

J.2.2.7 INFO message body parts

The MIME type of the message body carrying participant identities is application/vnd.3gpp.mcptt-info+xml. The application/vnd.3gpp.mcptt-info+xml MIME type is defined in 3GPP TS 24.379.

When associated with the g.3gpp.mcptt-info info package, the Content-Disposition value of the message body carrying mcptt information is "info-package".

J.2.2.8 Info package usage restrictions

None defined.

J.2.2.9 Rate of INFO Requests

Single INFO request generated after session set up.

J.2.2.10 Info package security considerations

The security is based on the generic security mechanism provided for the underlying SIP signalling. No additional security mechanism is defined.

J.2.2.11 Implementation details and examples

UAC generation of INFO requests: See 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification".

UAS processing of INFO requests: See 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification"

EXAMPLE: A controlling MCPTT function will receive a SIP INVITE request or SIP (re-)INVITE request containing a request for an emergency call (with or without an alert) or an imminent peril call. When an emergency call has been authorised but an optional request for an emergency alert has been determined to be unauthorised, the controller will respond with a SIP 200 (OK) response to indicate acceptance of the call request and return an indication of the rejection of the emergency alert request in a SIP INFO request carrying the application/vnd.3gpp.mcptt-info+xml MIME body using the g.3gpp.mcptt-info info package.

Annex K (informative): IANA UDP port registration form

This annex contains information to be provided to IANA for MCPTT Off-Network Protocol (MONP) UDP port registration. The following information is to be used to register MONP user port number and service name in the "IANA Service Name and Transport Protocol Port Number Registry" and specifically "Service Name and Transport Protocol Port Number Registry". This registration form can be found at: https://www.iana.org/form/ports-services.

Assignee Name	<MCC name>
Assignee E-mail	<MCC email address>
Contact Person	<MCC name>
Contact E-mail	<MCC email address>
Resources required	Port number and service name
Transport Protocols	UDP
Service Code	
Service Name	3gpp-monp
Desired Port Number	
Description	Mission Critical Push To Talk over LTE (MCPTT) Off-Network Protocol (MONP) is a 3GPP control protocol used by a MCPTT client hosted on a User Equipment (UE). MONP facilitates the MCPTT public safety service between MCPTT clients hosted on UEs communicating using IP using a single physical network segment, separated from Internet and any other IP network. The network segment is wireless network segment and UEs are mobile devices. The MCPTT public safety service offers half-duplex voice communication.
Reference	3GPP TS 24.379
Defined TXT keys	N/A
If broadcast/multicast is used, how and what for?	When performing off-network group calls, the MCPTT client initiates the group call to an MCPTT Group by sending a group call announcement message. The group call announcement message is a Mission Critical Push To Talk over LTE (MCPTT) Off-Network Protocol (MONP) message which is sent as a UDP message to a multicast IP address of the MCPTT group so that it is ensured that the MONP messages sent for the corresponding MCPTT group are only received by the MCPTT group's members.
If UDP is requested, please explain how traffic is limited, and whether the protocol reacts to congestion.	The number of Mission Critical Push To Talk over LTE (MCPTT) Off-Network Protocol (MONP) messages that need to be sent between MCPTT clients depends upon the number of members of the MCPTT group. MONP employs a back-off mechanism to defer transmission of another MONP message once a MONP message is received. MONP controls the number of messages transmitted within a certain, configurable amount of time, thus averting congestion. At maximum a few MONP messages per second are expected in communication between MCPTT clients. MONP does not support any reaction to congestion.
If UDP is requested, please indicate whether the service is solely for the discovery of hosts supporting this protocol.	Mission Critical Push To Talk over LTE (MCPTT) Off-Network Protocol (MONP) is not used solely for discovery of hosts supporting this protocol.

Please explain how your protocol supports versioning.	Mission Critical Push To Talk over LTE (MCPTT) Off-Network Protocol (MONP) does not support versioning.
If your request is for more than one transport, please explain in detail how the protocol differs over each transport.	N/A
Please describe how your protocol supports security. Note that presently there is no IETF consensus on when it is appropriate to use a second port for an insecure version of a protocol.	Mission Critical Push To Talk over LTE (MCPTT) Off-Network Protocol (MONP) does not support security. MONP relies on the security mechanisms of the lower layers.
Please explain why a unique port assignment is necessary as opposed to a port in range (49152-65535) or existing port.	As a general principle, 3GPP protocols use assigned User Ports, e.g. GTP-C uses UDP port number 2123, GTP-U uses UDP port number 2152, S1AP uses SCTP port number 36412, X2AP uses SCTP port number 36422, WLCP uses 36411. A dynamic port number (i.e. 49152 to 65535) cannot be used for the Mission Critical Push To Talk over LTE (MCPTT) Off-Network Protocol (MONP) because of the nature of communication on a single physical network segment, separated from Internet and any other IP network. The requirement of MONP to continuously listen for incoming messages needs an always active listener port. There is no local server that is administering the use of emphemeral ports in the MONP architecture, so there would be no way for one MCPTT client to know that a port is already being used by another MCPTT client. Communication can potentially be long-lived and MCPTT clients could leave and re-join the calls.
Please explain the state of development of your protocol.	Protocol Standard definition. No implementation exists yet.
If SCTP is requested, is there an existing TCP and/or UDP service name or port number assignment? If yes, provide the existing service name and port number.	N/A
What specific SCTP capability is used by the application such that a user who has the choice of both TCP (and/or UDP) and SCTP ports for this application would choose SCTP? See RFC 4960 section 7.1.	N/A
Please provide any other information that would be helpful in understanding how this protocol differs from existing assigned services	This protocol is between the UEs communicating using IP over a single physical network segment, separated from Internet and any other IP network. An MCPTT public safety service offered by the MCPTT clients hosted by the UEs is for public safety. The MCPTT public safety service offers half-duplex voice communication. This differs from existing protocols in 3GPP where UDP ports have been requested, as those protocols have been either between the UE and network or between network elements.

Annex L (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2015-07					Initial version.	-	0.0.0
2015-08					Implementation of the following P-CRs from CT1#92-bis MCPTT: C1ah-150007; C1ah-150042; C1ah-150046	0.0.0	0.1.0
2015-08					Implementation of the following P-CRs from CT1#93: C1-152952; C1-152956; C1-153125; C1-153177; C1-153178; C1-153179; C1-153180; C1-153220; C1-153229 ;changes by Rapporteur	0.1.0	0.2.0
2015-08					Minor fixes from the rapporteur	0.2.0	0.2.1
2015-09					Modifying the cover sheet to add the TS number and replacing MCPTT TS references with their allocated numbers. Changes by the rapporteur.	0.2.1	0.2.2
2015-10					Implementation of the following P-CRs from CT1#94: C1-153730; C1-153736; C1-153739; C1-153740; C1-154748; C1-153749; C1-153750; C1-153751; C1-153762;C1-153763; C1-153764; C1-153765; C1-153766; C1-153802; C1-153804; C1-153805; C1-153926; C1-153975;	0.2.2	0.3.0
2015-11					Implementation of the following P-CRs from CT1#95: C1-154472; C1-154473; C1-154326; C1-154480; C1-154103; C1-154477; C1-154478; C1-154479; C1-154858; C1-154355; C1-154398; C1-154535; C1-154536; C1-154537; C1-154539; C1-154540; C1-154542; C1-154544; C1-154548; C1-154549; C1-154550; C1-154552; C1-154553; C1-154712; C1-154715; C1-154716; C1-154717; C1-154731; C1-154732;C1-154399; C1-154401; Editorial changes by rapporteur.	0.3.0	0.4.0
2015-11					Minor editorial fixes from the rapporteur	0.4.0	0.4.1
2015-12	CT-70	CP-150733			Version 1.0.0 created for presentation for information	0.4.1	1.0.0
2016-01					Implementation of the following P-CRs from CT1#95-bis: C1-160322; C1-160323; C1-160326; C1-160380; C1-160392; C1-160393; C1-160394; C1-160395; C1-160396, C1-160397; C1-160400; C1-160414; C1-160415; C1-160416; C1-160417; C1-160418; C1-160419; C1-160420; C1-160421; C1-160422; C1-160423; C1-160453, C1-160455; C1-160456; C1-160457; C1-160458; C1-160466; C1-160489; C1-160490; C1-160491; C1-160612; C1-160617; C1-160770; Editorial changes by rapporteur.	1.0.0	1.1.0
2016-02					(1) Implementation of the following P-CRs from CT1 MCPTT-adhoc: C1ah-160039; C1ah-160074; C1ah-160075; C1-ah160080; C1ah-160083; C1ah-160100; C1ah-160101; C1ah-160102; C1ah-160107; C1ah-160108; (2) Implementation of the following P-CRs from CT1#96: C1-161042; C1-161045; C1-161047; C1-161048; C1-161050; C1-161058; C1-161108; C1-161109; C1-161139; C1-161206; C1-161208; C1-161209; C1-161212; C1-161213; C1-161214; C1-161234; C1-161302; C1-161304; C1-161305; C1-161308; C1-161312; C1-161357; C1-161358; C1-161359; C1-161360; C1-161361; C1-161364; C1-161366; C1-161367; C1-161368; C1-161369; C1-161389; C1-161390; C1-161391; C1-161393; C1-161394; C1-161395; C1-161396; C1-161438; C1-161439; C1-161440; C1-161441; C1-161505; C1-161507; C1-161508; C1-161512; C1-161520; C1-161521. (3) Editorial changes by rapporteur.	1.1.0	1.2.0

2016-02					Further corrections by rapporteur	1.2.0	1.2.1
2016-03	CT-71	CP-160059			Version 2.0.0 created for presentation for approval	1.2.1	2.0.0
2016-03	CT-71				Version 13.0.0 created after approval	2.0.0	13.0.0
2016-03					Minor editorial changes from TS rapporteur	13.0.0	13.0.1
2016-06	CT-72	CP-160322	0001	1	Subscription to the conference package	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0011		Removing editor's note about MBMS and broadcast group call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0002	1	Triggering conference event subscription – controlling MCPTT function	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0003	1	Triggering conference event subscription – non-controlling MCPTT function	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0004	1	Triggering conference event subscription – MCPTT client	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0005	1	Rejoin, join or late entry procedures added in non-controlling MCPTT function	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0006	1	Clarifying SDP procedures	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0007	1	Cleaning the usage of multipart/mixed content type	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0008	1	URIs in SIP responses clarification	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0010	3	Automatic commencement for On-Demand session clarifications	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0012	1	Automatic commencement for pre-established session clarification	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0013		Removing text about REFER in controlling MCPTT function	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0014	3	Manual Commencement Mode corrections	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0015		Correcting the use of <mcptt-calling-group-id>	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0016		Removing isfocus in responses from non-controlling MCPTT function	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0017	4	Temporary group flows as a result of group regrouping	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0018	1	Corrections in affiliation procedures	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0019	5	Corrections to call control	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0020	3	24.379 rel-13 Off-network Call Merge	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0021	2	24.379 rel-13 Off-network Emergency alert	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0022		Off-network implicit downgrade timer	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0023	2	24.379 rel-13 Off-network mandatory floor control in private calls	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0024	2	24.379 rel-13 Off-network message format alignment	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0025	3	24.379 rel-13 Off-network editor's notes	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0026	2	Corrections to clauses 4 to 12	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0028	2	Location procedures edits and cross reference fix	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0030	2	MBMS corrections	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0032	2	Annex B corrections	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0035	1	Alignment of XML schema for extensibility	13.0.1	13.1.0

2016-06	CT-72	CP-160322	0034	1	The meaning of the word, see, when used in F.3.3	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0036	1	MIME body corrections	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0037	2	Annex H corrections and modifications	13.0.1	13.1.0
2016-06	CT-72	C1-162029	0038	1	MCPTT Session Identity clarification	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0039		Replace the use of "this document" with "the present document"	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0040	2	Correct the specification of the acknowledged call setup timer	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0041	2	Correct the specification of the in-progress emergency group call timer.	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0042		Compliance Statement	13.0.1	13.1.0
2016-06	CT-72	CP-160342	0043	3	Correct authorisation to join a group call or initiate a group call.	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0044		Affiliation Check	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0045	2	Modifications to use of non-controlling function	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0046		Private Call Corrections	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0047	1	Setting the P-Asserted-Identity in responses from the terminating participating MCPTT function.	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0048		Remove privacy requirements using SIP Privacy header field	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0049	4	Out of dialog REFER and no implicit subscription.	13.0.1	13.1.0
2016-06	CT-72	CP-160343	0050	3	MCPTT identities used in pre-established sessions	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0051		Correct the encoding of the "purpose tag" in the PCK.	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0052		Functional description of MONP	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0053	5	General procedure for confidentiality protection of specific XML elements.	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0054	4	General procedure for integrity protecting XML documents	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0055	3	Corrections to SIP PUBLISH	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0056	5	Descriptive text on MCPTT emergency alert subclause 4.6.3	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0057	5	Emergency alert client procedures	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0058	3	Emergency alert participating and controlling function procedures	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0059	4	Descriptive text on MCPTT imminent peril call Subclause 4.6.4	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0060	4	Client originating procedures for on-demand priority calls	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0061	4	Participating MCPTT functions modifications for on-demand priority calls and alerts	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0062	5	Chat controlling function emergency and imminent peril updates	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0063	4	MCPTT prearranged controlling function updates for emergency and imminent peril origination	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0064	4	Terminating MCPTT client receives a SIP INVITE request or SIP re-INVITE for an MCPTT group call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0065	3	Origination MCPTT client SIP REFER updates for MCPTT emergency and imminent peril group calls	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0067	4	Descriptive text on MCPTT emergency private call - subclause 4.6.2	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0068	4	Description of imminent peril states	13.0.1	13.1.0

2016-06	CT-72	CP-160322	0070	2	Definition of content for the User location IE and removal of EN	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0071		Removing several editor's note	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0073	4	Alignment of commencement mode determination with answer mode settings delivered by the MCPTT client	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0075	1	Correcting MCPTT address to MCPTT ID	13.0.1	13.1.0
2016-06	CT-72	CP-160359	0076	3	P-Asserted-Identity added in the Referred-By header field	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0077	1	mcptt-group-id changed to mcptt-calling-group-id in annex H	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0078	1	Changing from 2xx to 200 OK when sending a response	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0079	1	Hiding of the MCPTT ID in MBMS listening status report	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0080	1	MBMS usage procedure error corrections	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0082	2	O-PF private call authorisations for on-demand call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0083	2	Alignment of XML schemas in annex F of 24.379	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0084	1	O-PF group call authorisations commencement mode actions	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0085	1	T-PF private call commencement mode for on-demand call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0086	1	T-PF group call commencement mode for on-demand call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0087	1	Originating client private call modifications for on-demand call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0088	1	Terminating client private call modifications for on-demand call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0089	1	Terminating client group call modifications for on-demand call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0090	1	Maximum number of simultaneously received group calls (N6)	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0091		Referring to on-network-max-participant-count in TS 24.381	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0092		Correcting names of XML elements "disabled" and "invite-members"	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0093		Correcting name of "required" XML element	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0094	1	Missing procedures of originating PF of authorized MCPTT user	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0095	1	The g.3gpp.icsi-ref media feature tag included in the Contact header field	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0096	2	Clarifications on calling a temporary group	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0097	1	Adding use of "preferred-voice-encodings" to SDP procedures	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0098		Adding use of "on-network-minimum-number-to-start" element to group procedures	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0099	1	Implementing conditions for maximum duration of on-network group call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0100	1	Handling the current speaker during group regrouping	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0101	1	MBSFN Area Id: Alt-1 (Removal from call control specification)	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0103	1	MCPTT client origination procedures for on-demand private emergency call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0104	1	MCPTT client termination procedures for on-demand private emergency call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0105	1	MCPTT participating function procedures for private emergency call	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0106	1	MCPTT controlling function procedures for private emergency call	13.0.1	13.1.0

2016-06	CT-72	CP-160322	0107		Correcting subsequent request procedures	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0108	1	Switching from MBMS bearer to unicast bearer based on MBMS listening status	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0110	2	Completion of Pre-established Session General	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0111	2	Completion of Pre-established Session Establishment	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0112	3	Completion of Pre-established Session Modification	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0122		MBMS Service Area ID alignment	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0114	2	Pre-established Session Release	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0115	1	Off-network - Corrections to private call security context	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0116	1	Off-network - Correction to state machines	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0117	1	Off-network - Corrections to timers and counters.	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0118		Removal of unused warning texts from subclause 4.4.2	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0119		Description of emergency private call states	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0120		MCPTT server procedures for prearranged priority call re-INVITEs	13.0.1	13.1.0
2016-06	CT-72	CP-160322	0123		Reference number not implemented	13.0.1	13.1.0
2016-06	CT-72				Various corrections	13.1.0	13.1.1
2016-09	CT-73	CP-160439	0125	2	Emergency group call cancel procedure updates for authorised users	13.1.1	13.2.0
2016-09	CT-73	CP-160556	0126	2	MCPTT state management and authorisation corrections for priority calls	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0127	1	Introducing priority sharing in participating MCPTT function	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0128	1	Resolving an editor's note about broadcast group call	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0129	1	Terminating subscription to the event package	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0130	1	Removing errors in re-INVITE and UPDATE procedures	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0131		Authorizing MCPTT clients in constituent groups in non-controllers that do not expose group members, when initiating a temporary group session	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0132	1	Clarifying the sending of SIP NOTIFY request during release of temporary group call	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0133	1	Updating the release policy for chat group	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0134		Moving overriding speaker - call control part	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0135	2	Pre-established session functionality for emergency and imminent peril calls.	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0136		MCPTT client ID	13.1.1	13.2.0
2016-09	CT-73	CP-160498	0137	2	Confidentiality of URIs in XML attributes	13.1.1	13.2.0
2016-09	CT-73	CP-160557	0139	2	Removal of Editor's Notes related to emergency functionality and possible optimizations	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0140		Resolution of Editor's Notes related to priority mechanisms	13.1.1	13.2.0
2016-09	CT-73	CP-160504	0141	2	Assignment of Resource Priority header field values	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0143		EN: Coding of <Configuration> element	13.1.1	13.2.0
2016-09	CT-73	CP-160499	0144	1	EN: Reference regarding mission critical organization.	13.1.1	13.2.0

2016-09	CT-73	CP-160497	0145	1	EN: Resource-Share and INVITE without SDP	13.1.1	13.2.0
2016-09	CT-73	CP-160514	0146		Reference update draft-holmberg-dispatch-mcptt-rp-namespace	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0147		Update the use of configuration for signalling protection	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0148	1	Description of encryption of elements and attributes in pre-established sessions	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0149		Admitting a higher priority user to a call that has reached its max users	13.1.1	13.2.0
2016-09	CT-73	CP-160440	0150	1	Emergency Indications currently in SIP 200 (OK) to SIP INVITE requests need to be in SIP INFO requests	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0151		Corrections for max simultaneous sessions	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0152	1	Solving general editor's notes and removing solved editor's notes	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0153		Removal of editor's notes related to id hiding	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0154		Management of media resource allocation for pre-established sessions	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0155		Remove privacy requirements from Rel-13 MCPTT	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0156		XML schema changes to accommodate confidentiality protection	13.1.1	13.2.0
2016-09	CT-73	CP-160498	0157	2	XML schema changes to accommodate integrity protection	13.1.1	13.2.0
2016-09	CT-73	CP-160542	0158	5	MCPTT Service Continuity	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0160	2	IP address and port number for media stream	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0162	1	Authorization checks	13.1.1	13.2.0
2016-09	CT-73	CP-160496	0163		Removal of editor's note on call probe	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0165	1	Max duration of the calls	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0166		Restrict notification of call failure reason for private call	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0167	1	Timer TFB3	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0168	1	IANA Registration form for UDP Port number for MONP messages	13.1.1	13.2.0
2016-09	CT-73	CP-160497	0169		Error in authorization reference	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0170	2	MCPTT session identity and subscription to conference events	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0171	3	Completion of Pre-established session	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0172	1	Resolution of Editor's Note on NATs	13.1.1	13.2.0
2016-09	CT-73	CP-160500	0176		Downloading MCPTT user profile when receiving the service settings	13.1.1	13.2.0
2016-09	CT-73	CP-160558	0177		Alignment with MCPTT user profile document in TS 24.384	13.1.1	13.2.0
2016-12	CT-74	CP-160731	0178		Addition of MCPTT client id to SIP requests, correction of <originated-by> XML element definition	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0179		Missing user info entry addition	13.2.0	13.3.0
2016-12	CT-74	CP-160756	0180	4	Corrections for missing implicit affiliation functionality	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0181	1	MBMS transmission usage procedure corrections	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0182		Modify emergency authorisations	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0183	1	Broadcast group calls	13.2.0	13.3.0

2016-12	CT-74	CP-160732	0184		Solving Editor's Notes on Priority	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0185		Implicit Floor Request sent in Re-INVITE requests	13.2.0	13.3.0
2016-12	CT-74	CP-160732	0187	4	Transport MKFC from CF to PF in session set-up	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0189	4	SAI and QCI in the MBMS announcement	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0191		Reference update draft-holmberg-dispatch-mcptt-rp-namespace	13.2.0	13.3.0
2016-12	CT-74	CP-160689	0193	2	Corrections to implicit downgrade timers	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0194	1	Handling the ARP of an MBMS bearer in emergency update	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0197	3	Identification of pre-selected MCPTT user profile at the MCPTT server	13.2.0	13.3.0
2016-12	CT-74	CP-160732	0198	1	SIP 403 should not indicate "partial success".	13.2.0	13.3.0
2016-12	CT-74	CP-160190	0199	3	Adding missing implicit affiliation at service authorisation	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0201		Correct Imminent Peril call perfect case state transistion	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0202	1	Corrections to broadcast group call state machine	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0203		Misinterpretations caused by UE roles in titles of subclauses in subclause 10.2.2.4	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0205	1	Priority call origination using pre-established sessions	13.2.0	13.3.0
2016-12	CT-74	CP-160731	0206	1	PF providing MSCCK and MSCCK-ID to served UEs	13.2.0	13.3.0
2012-09	CT-74	CP-160743	0142	1	Correction to SDP media level parameters for floor control in SIP signalling flows	13.3.0	14.0.0
2016-12	CT-74	CP-160743	0188		Inaccurate representation of application/vnd.3gpp.mcptt-signed+xml MIME body	13.3.0	14.0.0
2016-12	CT-74	CP-160743	0190		Key terminology clarifications	13.3.0	14.0.0
2016-12	CT-74	CP-160743	0196		When to send "not listening to the MBMS subchannels"	13.3.0	14.0.0
2016-12	CT-74	CP-160743	0204	1	Security related definitions	13.3.0	14.0.0
2017-03	CT-75	CP-170114	0208		Corrections in affiliation procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170114	0210		Correction of the tag name used for location	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0211	4	Distinction of requests at the MCPTT client and the MCPTT server for private call call-back	14.0.0	14.1.0
2017-03	CT-75	CP-170127	0212		Request-URI of incoming INVITE should not contain the IMPU	14.0.0	14.1.0
2017-03	CT-75	CP-170127	0213		Removal of redundant procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170115	0215		P-Asserted-Service missing from SIP MESSAGE requests from the controlling MCPTT function.	14.0.0	14.1.0
2017-03	CT-75	CP-170114	0217	1	Contact header field must not be included in SIP MESSAGE or in 2xx response to SIP MESSAGE.	14.0.0	14.1.0
2017-03	CT-75	CP-170115	0219	1	Message body must not be included in a 2xx response to SIP MESSAGE.	14.0.0	14.1.0
2017-03	CT-75	CP-170127	0220		Corrections to Appendix H.3	14.0.0	14.1.0
2017-03	CT-75	CP-170115	0221	1	Corrections to user location	14.0.0	14.1.0
2017-03	CT-75	CP-170114	0223	1	Corrections to SIP NOTIFY	14.0.0	14.1.0
2017-03	CT-75	CP-170127	0224	1	Modifying references in TS 24.379 to cater for rel-14 Stage 1, 2 and Stage 3 mission critical restructure	14.0.0	14.1.0
2017-03	CT-75	CP-170115	0228	1	Reference update draft-holmberg-dispatch-mcptt-rp-namespace	14.0.0	14.1.0

2017-03	CT-75	CP-170125	0229	1	Private Call Call-Back general procedures and client procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0230	1	Private Call Call-Back PF procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0231	1	Private Call Call-Back CF procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0232	1	Private Call Call-Back states in the UE	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0233	1	Private Call Call-Back XML modifications	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0236		First-to-answer call XML modifications	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0237	1	First-to-answer call client procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170070	0238	2	First-to-answer call participating function procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0239	1	First-to-answer call controlling function procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170069	0241	2	Removal of bodies from 200 OK messages sent from the terminating client	14.0.0	14.1.0
2017-03	CT-75	CP-170115	0242	1	SIP 200 (OK) to SIP INFO request not specified	14.0.0	14.1.0
2017-03	CT-75	CP-170127	0243	1	Removal of "hanging paragraphs" and other editorials	14.0.0	14.1.0
2017-03	CT-75	CP-170114	0244	1	The wrong steps are referenced in procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170115	0245	1	Resource-Priority header should not be included in SIP MESSAGE.	14.0.0	14.1.0
2017-03	CT-75	CP-170127	0246	1	Terminology of "join", "initiates", "establishes" and "re-join" needs to be explained	14.0.0	14.1.0
2017-03	CT-75	CP-170127	0247	1	Replace "this MCPTT user" with "the MCPTT user"	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0248	2	Ambient listening call client originating procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0249	2	Ambient listening call client release procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0250	2	Ambient listening call participating function procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0251	2	Ambient listening call controlling function procedures	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0252	1	Ambient listening call definitions	14.0.0	14.1.0
2017-03	CT-75	CP-170125	0253	1	Ambient listening xml changes	14.0.0	14.1.0
2017-03	CT-75	CP-170073	0254	2	Indicating the selected User Profile	14.0.0	14.1.0
2017-03	CT-75	CP-170114	0257		Correction of client usage of RPH	14.0.0	14.1.0
2017-03	CT-75	CP-170114	0259	1	Corrections to off-network emergency alert timers	14.0.0	14.1.0
2017-03	CT-75	CP-170056	0260		Correction of mislabeled states	14.0.0	14.1.0
2017-03	CT-75	CP-170127	0262		Correction of timer name for offnetwork emergency alert	14.0.0	14.1.0
2017-03	CT-75	CP-170240	0267	1	"monp" already used as a service-name in the IANA Service Name and Transport Protocol Port Number Registry	14.0.0	14.1.0
2017-03	CT-75	CP-170210	0269		Issue found with existing IANA XML MIME type registration forms in TS 24.379	14.0.0	14.1.0

Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-06	CT-76	CP-171066	0272	1	A	Correction for imminent peril cancellation	14.2.0
2017-06	CT-76	CP-171066	0274	1	A	Correction of emergency alert cancellation procedures	14.2.0
2017-06	CT-76	CP-171079	0275	1	F	Correction of FTAC emergency handling for terminating clients	14.2.0
2017-06	CT-76	CP-171066	0277		A	Missing chat session release procedures and corrected release policy	14.2.0

2017-06	CT-76	CP-171079	0278	2	B	Client procedures for ambient listening call using pre-established sessions	14.2.0
2017-06	CT-76	CP-171079	0279	2	B	Participating function procedures for ambient listening call using pre-established sessions	14.2.0
2017-06	CT-76	CP-171079	0280	4	B	Client procedures for remote change of selected group	14.2.0
2017-06	CT-76	CP-171079	0281	3	B	Participating function procedures for remote change of selected group	14.2.0
2017-06	CT-76	CP-171079	0282	3	B	Controlling function procedures for remote change of selected group	14.2.0
2017-06	CT-76	CP-171066	0284		A	Reference update draft-holmberg-dispatch-mcptt-rp-namespace	14.2.0
2017-06	CT-76	CP-171079	0287	1	B	Ambient listening on-demand client authorisation procedures	14.2.0
2017-06	CT-76	CP-171079	0288	1	B	Ambient listening on-demand PF authorisation procedures	14.2.0
2017-06	CT-76	CP-171066	0290		A	Corrections to mcpttinfo schema	14.2.0
2017-06	CT-76	CP-171093	0291	2	B	Response-Source header field handling completion	14.2.0
2017-06	CT-76	CP-171066	0293	1	A	Corrections to off-network private call	14.2.0
2017-06	CT-76	CP-171079	0294	1	B	Floor control updates for ambient listening call	14.2.0
2017-06	CT-76	CP-171066	0296		A	Correction of priority call request validation	14.2.0
2017-06	CT-76	CP-171079	0297	2	B	MBMS bearer suspension	14.2.0
2017-06	CT-76	CP-171079	0298	1	B	Update of AL server-initiated release	14.2.0
2017-06	CT-76	CP-171079	0299	1	B	Addition of authorisation checks for FTAC	14.2.0
2017-06	CT-76	CP-171079	0300	2	F	Implementation of CSK 'key download' procedure	14.2.0
2017-06	CT-76	CP-171079	0302	1	C	Correct and align MCPTT Registration and Service Authorisation procedure with MCVideo and MCData	14.2.0
2017-06	CT-76	CP-171066	0304	3	A	Resource Sharing with pre-established sessions	14.2.0
2017-06	CT-76	CP-171079	0307	1	F	Introduction of KMS URI	14.2.0
2017-06	CT-76	CP-171066	0309		A	Correct (De-)affliation schema	14.2.0
2017-09	CT-77	CP-172093	0311		A	Correction of missing mcptt-client-id in SIP REGISTER	14.3.0
2017-09	CT-77	CP-172101	0312		B	Addition of eMCPTT definitions	14.3.0
2017-09	CT-77	CP-172101	0313	2	F	Key management for first-to-answer call	14.3.0
2017-09	CT-77	CP-172093	0315		A	Terminating procedure for Re-join corrected	14.3.0
2017-09	CT-77	CP-172093	0317		A	Missing procedures and incorrect referencing for private call client procedures	14.3.0
2017-09	CT-77	CP-172093	0320	1	A	Last call type change time	14.3.0
2017-09	CT-77	CP-172093	0322	1	A	Stored call start time of the call	14.3.0
2017-09	CT-77	CP-172093	0324		A	tCoordinateType	14.3.0
2017-09	CT-77	CP-172094	0326	1	A	Timer TFG13	14.3.0
2017-09	CT-77	CP-172093	0328		A	Key-mgmt attribute	14.3.0
2017-09	CT-77	CP-172093	0330		A	SDP for Private call	14.3.0
2017-09	CT-77	CP-172094	0334	3	A	Essential correction to MBMS Bearer Announcement Message	14.3.0
2017-09	CT-77	CP-172101	0335	2	F	Send one MBMS Bearer Announcement Message per TMGI intended for GPMS	14.3.0
2017-09	CT-77	CP-172094	0336			Corrections to off-network call control procedures	14.3.0
2017-09	CT-77	CP-172093	0338	1	A	Coding Error ABNF for the Warning text	14.3.0
2017-09	CT-77	CP-172094	0340	1	A	Correction of state naming for MIG 3, and MIG 4	14.3.0
2017-09	CT-77	CP-172093	0342		A	Correction of identifier mcptt calling user id	14.3.0
2017-09	CT-77	CP-172094	0344	1	A	Correction of identifier for <imminentperil-ind>	14.3.0
2017-09	CT-77	CP-172094	0346	1	A	Correction of cross referenced steps	14.3.0
2017-09	CT-77	CP-172101	0349	1	B	KMS URI update for off network operations	14.3.0
2017-09	CT-77	CP-172094	0351	1	A	Addition of Registration without Auth Token	14.3.0
2017-09	CT-77	CP-172101	0353	1	F	MBMS Bearer Management by the MCPTT participation function	14.3.0
2017-12	CT-78	CP-173063	0358		F	Replace obsolete references to 33.179 with updated references to 33.180	14.4.0
2017-12	CT-78	CP-173063	0359		F	Introduction of MuSiK for alignment with Rel-14 security procedures	14.4.0
2017-12	CT-78	CP-173063	0360	2	F	Removal of MKFC processing as part of replacing MKFC wit h MuSiK	14.4.0
2017-12	CT-78	CP-173053	0361	2	A	Addition of missing warning code 136 for I_MESSAGE authentication failure	14.4.0
2017-12	CT-78	CP-173053	0363	1	A	Correction and clarification of XML integrity protection	14.4.0
2017-12	CT-78	CP-173053	0365	1	A	Location correction for emergency alert	14.4.0
2017-12	CT-78	CP-173053	0367	1	A	Off-network call type control procedures: merge of two calls	14.4.0
2017-12	CT-78	CP-173053	0368	1	A	Off-network Broadcast group call procedures	14.4.0
2017-12	CT-78	CP-173053	0372		A	Four most significant bits of PCK-ID	14.4.0

History

Document history		
V14.1.0	April 2017	Publication
V14.2.0	July 2017	Publication
V14.3.0	October 2017	Publication
V14.4.0	January 2018	Publication