ETSI TS 129 379 V16.3.0 (2021-10)

LTE;
5G;
Mission Critical Push To Talk (MCPTT)
call control interworking with Land Mobile Radio (LMR)
systems;
Stage-3
(3GPP TS 29.379 version 16.3.0 Release 16)

Reference
RTS/TSGC-0129379vg30

Keywords
5G,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 normative deliverables 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.

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

In the present document, certain modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

NOTE 1: The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

NOTE 2: The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

NOTE 3: The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

NOTE 4: The constructions "can" and "cannot" shall not to be used as substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

NOTE 5: The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies the call control protocols needed to support a Mission Critical Push To Talk (MCPTT) system interworking with a Land Mobile Radio (LMR) system.

The IWF supports the basic group and other features as specified in 3GPP TS 23.283 [28]. The present document describes functionality modelled on 3GPP TS 24.379 [29].

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 23.379: "Functional architecture and information flows to support mission critical communication services; Stage 2".

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

[4] 3GPP TS 24.380: "Mission Critical Push To Talk (MCPTT) floor control Protocol specification".

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

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

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

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

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

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

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

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

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

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

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

[16] 3GPP TS 24.481: "Mission Critical Services (MCS) group management Protocol specification".

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

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

[19] 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".

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

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

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

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

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

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

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

[27] 3GPP TS 33.180: "Security of the mission critical service".

[28] 3GPP TS 23.283: "Mission Critical Communication Interworking with Land Mobile Radio Systems; Stage 2".

[29] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification".

[30] 3GPP TS 24.282: "Mission Critical Data (MCData) signalling control; Protocol specification".

[31] 3GPP TS 29.380: "Mission Critical Push To Talk (MCPTT) media plane control interworking with LMR systems".

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

[33] 3GPP TS 29.582: "Mission Critical Data (MCData) interworking with LMR systems".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms 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].

IWF performing the controlling role: an IWF role in which the IWF interacts with MCPTT participating functions and MCPTT non-controlling functions across the IWF-1 interface.

IWF performing the non-controlling role: an IWF role in which the IWF interacts with MCPTT participating functions and MCPTT controlling functions across the IWF-1 interface

IWF performing the participating role: an IWF role in which the IWF interacts with MCPTT controlling functions and MCPTT non-controlling functions across the IWF-1 interface.

Participant homed in the IWF: same as "User homed in the IWF".

User homed in the IWF: A user represented by an MCPTT ID in the IWF with the same domain as the IWF.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.283 [28] apply:

Interworking Function (IWF)

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].

IWF	InterWorking Function
KMS	Key Management Service
LMR	Land Mobile Radio
MC	Mission Critical
MCPTT	Mission Critical Push To Talk
URI	Uniform Resource Identifier

4 General

4.1 IWF overview

The IWF interacts with the controlling, participating and non-controlling MCPTT functions of an MCPTT system as a peer system via the IWF-1 interface and with MCData systems via the IWF-2 interface. The IWF supports a subset of the client-server group management interfaces defined in 3GPP TS 24.481 [16] required to support IWF-3, with the exceptions and additions defined in the present document.

4.2 Warning Header Field

4.2.1 General

An IWF can include a free text string in a SIP response to a SIP request. When the IWF 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 [14]. The IWF includes the Warning code set to 399 (miscellaneous warning) and includes the host name set to the host name of the IWF.

4.2.2 Warning texts

Existing warning texts as specified in 3GPP TS 24.379 [29] will be used.

4.3 MCPTT priority calls and alerts

Clauses 4.6.1, 4.6.2, 4.6.3 and 4.6.4 in 3GPP TS 24.379 [29] describe the aspects and states that are key in managing priority calls and alerts.

The IWF manages the states on behalf of its homed users. For states that are managed by clients, the IWF manages an instance of the state for each client homed in the IWF.

4.4 Media security at the IWF

With respect to LMR interworking, the IWF provides the interfaces as specified in 3GPP TS 23.283 [28] and 3GPP TS 33.180 [27] to key management and group management capabilities of the LMR system.

4.5 Broadcast group calls

See 3GPP TS 24.379 [29] for a description of broadcast group calls.

5 Functional entities

5.1 General

An IWF can perform the controlling role for group calls and private calls. The controlling role serves as the group home, managing the floor and tracking group affiliations.

An IWF can perform the participating role for group calls and private calls. The participating role serves as the user home, checking user authorizations and forwarding signalling and media between the controlling role and clients.

An IWF can perform a non-controlling role for temporary group calls involving groups from multiple MCPTT systems. The non-controlling role serves as the controlling role for a constituent group of a regroup and coordinates with the controlling server of the temporary group.

An IWF performing the participating role can serve an originating LMR user. How the IWF serves LMR users is out of scope of 3GPP.

An IWF performing the participating role can serve a terminating LMR user. How the IWF serves LMR users is out of scope of 3GPP.

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

The same IWF 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 IWF acting in a participating role, the term, "IWF performing the participating role" is used.

When referring to the procedures in the present document for the IWF acting in a controlling role, the term "IWF performing the controlling role" is used.

When referring to the procedures in the present document for the IWF acting in a non-controlling role for a group call, the term " IWF performing the non-controlling role " is used.

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

- support the IWF procedures defined in 3GPP TS 23.283 [28];
- generate SDP offer and SDP answer in accordance with 3GPP TS 24.229 [3] and clause 6.3 of 3GPP TS 24.379 [29];
- implement the role of a centralised floor control server and implement the on-network procedures for floor control as specified in 3GPP TS 29.380 [31];
- for registration and service authorisation, IWF procedures are out of scope of the present document;
- for affiliation of users hosted in the MCPTT system, implement the procedures specified in the present document; for LMR users, the affiliation process is out of scope of the present document;
- for group call functionality (including broadcast, emergency and imminent peril), implement the procedures specified in the present document; and
- for private call functionality (including emergency), implement the procedures specified in the present document.

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 [27], an IWF shall behave as an encryption endpoint on behalf of its LMR users.

NOTE: A scenario with the IWF acting as an encryption endpoint is not end to end encryption. End to end encryption with LMR users is out of scope of the present document, but some tools are provided to allow end to end encryption to be defined outside of 3GPP.

To be compliant with the procedures for confidentiality protection of XML elements in the present document, the IWF shall implement the procedures specified in clause 6.6.2 of 3GPP TS 24.379 [29].

To be compliant with the procedures for integrity protection of XML MIME bodies in the present document, the IWF shall implement the procedures specified in clause 6.6.3 of 3GPP TS 24.379 [29].

5.2 Functional connectivity models

The following figures give an overview of the connectivity between the IWF and the MCPTT system with the IWF in different roles as described in clause 5.1.

NOTE: The MCPTT functional roles are not defined here. They are defined in 3GPP TS 24.379 [29] but are shown here to illustrate the relationship with the IWF.

Figure 5.2-1 shows the role of the IWF relative to an MCPTT system. Here, the controlling MCPTT function is in the MCPTT system and the called user is homed in the IWF. The IWF plays the role of the terminating participating function.

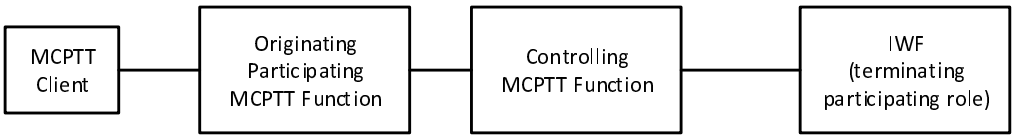

Figure 5.2-1: Relationship between the IWF and an MCPTT system with the controlling MCPTT function in the MCPTT system

Figure 5.2-2 shows the role of the IWF relative to an MCPTT system. Here, the controlling MCPTT function is in the MCPTT system and the calling user is homed in the IWF. The IWF plays the role of the originating participating function.

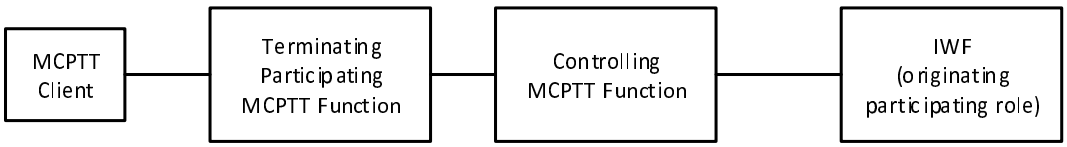

Figure 5.2-2: Relationship between the IWF and an MCPTT system with the controlling MCPTT function in the MCPTT system

Figure 5.2-3 shows the role of the IWF relative to an MCPTT system. Here, the controlling MCPTT function is in the IWF and the called user is homed in the IWF. The IWF plays the role of the controlling function.

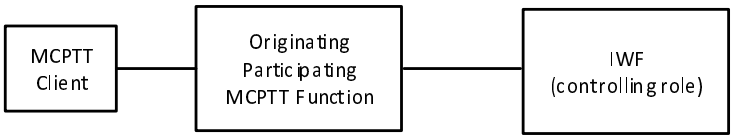

Figure 5.2-3: Relationship between the IWF and an MCPTT system with the controlling MCPTT function in the IWF

Figure 5.2-4 shows the role of the IWF relative to an MCPTT system. Here, the controlling MCPTT function is in the IWF and the calling user is homed in the IWF. The IWF plays the role of the controlling function.

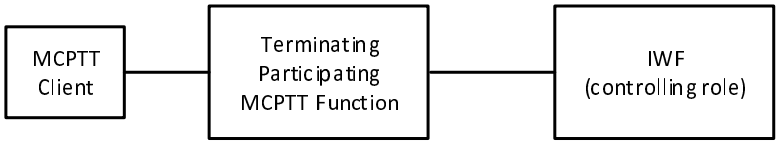

Figure 5.2-4: Relationship between the IWF and an MCPTT system with the controlling MCPTT function in the IWF

Figure 5.2-5 shows the role of the IWF relative to an MCPTT system. Here, the controlling MCPTT function is in the MCPTT system, the non-controlling function is in the IWF and the called user is homed in the IWF. The IWF plays the role of the non-controlling function.

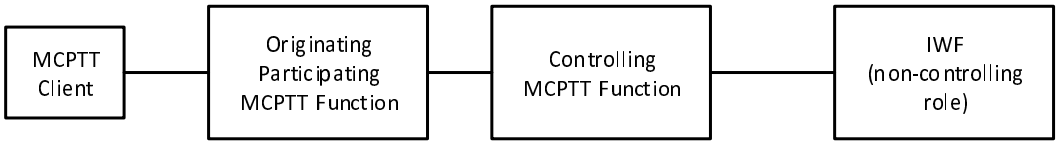

Figure 5.2-5: Relationship between the IWF and an MCPTT system with the controlling MCPTT function in the MCPTT system and a non-controlling function in the IWF

Figure 5.2-6 shows the role of the IWF relative to an MCPTT system. Here, the controlling MCPTT function is in the MCPTT system, the non-controlling function is in the IWF and the calling user is homed in the IWF. The IWF plays the role of the non-controlling function.

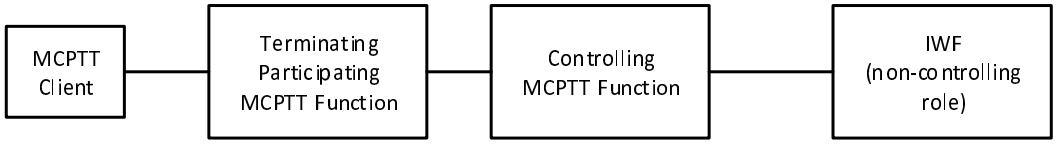

Figure 5.2-6: Relationship between the IWF and an MCPTT system with the controlling MCPTT function in the MCPTT system and a non-controlling function in the IWF

Other functional connectivity models can exist.

6 Call control common procedures

6.1 SDP

6.1.1 SDP offer generation

The SDP offer shall contain only one SDP media-level section for offered speech according to 3GPP TS 24.229 [3] 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 29.380 [31].

When composing an SDP offer according to 3GPP TS 24.229 [3] the IWF:

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

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;

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

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

      ii) if the <preferred-voice-encodings> element is present in the group document as specified in 3GPP TS 24.481 [16] containing an <encoding> element with a "name" attribute; and

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

      then the IWF shall insert the value of the "name" attribute in the <encoding name> field of the "a=rtpmap" attribute as defined in IETF RFC 4566 [8]; and

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

3) if floor control shall be used during the session, shall include an "m=application" media-level section as specified in 3GPP TS 29.380 [31] 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 29.380 [31]; and

   b) the 'fmtp' attributes as specified in 3GPP TS 29.380 [31] clause 14; and

4) if media security is required between the MCPTT client and the IWF for a private call, 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 [22].

6.1.2 SDP answer generation

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

When composing an SDP answer, the IWF:

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

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

NOTE: If the IWF 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 IWF 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 [3];

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 [3]; and

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 29.380 [31] clause 12; and

b) 'fmtp' attributes as specified in 3GPP TS 29.380 [31] clause 14.

6.2 Commencement modes

6.2.1 Automatic commencement mode for private calls

When performing the automatic commencement mode procedures, the IWF performing the participating role:

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

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 [6]. The "refresher" parameter in the Session-Expires header field shall be set to "uas";

6) 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 [3] with the clarifications given in clause 6.1.2;

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

8) shall interact with the media plane as specified in 3GPP TS 29.380 [31] clause 6.2.

6.2.2 Manual commencement mode for private calls

When performing the manual commencement mode procedures:

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

The IWF performing the participating role:

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

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 controlling MCPTT function.

When sending the SIP 200 (OK) response to the incoming SIP INVITE request, the IWF performing the participating role shall follow the procedures in clause 6.2.1.

6.3 Receiving an MCPTT session release request

Upon receiving a SIP BYE request, the IWF:

1) shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

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

6.4 Priority call conditions

6.4.1 MCPTT emergency group call conditions

6.4.1.1 SIP INVITE request for originating MCPTT emergency group calls

This clause is referenced from other procedures.

When the MCPTT emergency state is set, the IWF performing the participating role:

1) shall include in the application/vnd.3gpp.mcptt-info+xml MIME body in the SIP INVITE 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 IWF has determined that an MCPTT emergency alert is to be sent, 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 clause 6.5.1;

3) if the IWF has determined that an MCPTT emergency alert is not 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 user homed in the IWF of the group is set to a value other than "MEG 2: in-progress" set the MCPTT client emergency group state of the user homed in the IWF of the MCPTT group to "MEG 4: confirm-pending".

NOTE 1: This is the case of a user homed in the IWF 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 user homed in the IWF 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 IWF determines that the request for MCPTT emergency group call is authorized by local policy, the IWF performing the participating role 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 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 user homed in the IWF has also requested an MCPTT emergency alert to be sent, 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, if available, for MCPTT emergency alert as specified in clause 6.5.1;

3) if the IWF has determined that an MCPTT emergency alert is not 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 user homed in the IWF of the group is set to a value other than "MEG 2: in-progress" shall set the MCPTT client emergency group state of the user homed in the IWF 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 clause.

6.4.1.2 Resource-Priority header field for MCPTT emergency group calls

This clause 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", or the MCPTT client emergency group state of the group is set to "MEG 2: in-progress", the IWF performing the participating role shall include in the SIP INVITE request a Resource-Priority header field populated with the values for an MCPTT emergency group call as specified in clause 6.4.1.11.

NOTE: The IWF performing the participating role ideally would not need to maintain knowledge of the in-progress emergency state of the group (as tracked for the client by the MCPTT client emergency group state by the IWF performing the participating role) 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 the MCPTT client emergency group state of the group is "no-emergency" or "cancel-pending", the IWF performing the participating role shall include in the SIP INVITE request a Resource-Priority header field populated with the values for a normal MCPTT group call as specified in clause 6.4.1.11.

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

This clause 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 IWF performing the participating role shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [3] with the clarifications given below.

The IWF performing the participating role:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in 3GPP TS 24.379 [29], 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 1: This is the case of a user homed in the IWF 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 only the MCPTT emergency group call is to be cancelled, the IWF performing the participating role:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in 3GPP TS 24.379 [29], 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 2: This is the case of a user homed in the IWF that 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 user homed in the IWF has indicated that the MCPTT emergency alert on the MCPTT group should be cancelled in addition to the MCPTT emergency group call, the IWF performing the participating role:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in 3GPP TS 24.379 [29], clause F.1 with the <emergency-ind> element set to "false";

2) shall:

   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; and

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

NOTE 3: This is the case of a user homed in the IWF that has initiated both an MCPTT emergency group call and an MCPTT emergency alert and wishes to cancel both.

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

In the procedures in this clause, 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 IWF:

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 emergency group state of the user homed in the IWF of the group to "MEG 2: in-progress" if it was not already set;

   b) if the MCPTT emergency alert state of the user homed in the IWF 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 TS 24.379 [29] clause 4.4 with the warning text containing the mcptt-warn-code set to "149", shall set the MCPTT emergency alert state of the user homed in the IWF 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 TS 24.379 [29] clause 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".

6.4.1.5 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 clause, 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 IWF:

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 emergency group state of the user homed in the IWF of the group is "MEG 4: confirm-pending" shall set the emergency group state of the user homed in the IWF 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 of the user homed in the IWF 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".

6.4.1.6 SIP request for originating MCPTT imminent peril group calls

This clause is referenced from other procedures.

When the IWF performing the participating role determines to originate an MCPTT imminent peril group call, the IWF performing the participating role:

1) if the client homed in the IWF's 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 an application/vnd.3gpp.mcptt-info+xml MIME body as defined in 3GPP TS 24.379 [29], clause 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 client homed in the IWF's imminent peril group state of the group is set to a value other than "MIG 2: in-progress" shall set the client homed in the IWF's 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 client by the client imminent peril group state) will also have the priority associated with MCPTT imminent peril group calls. The <imminentperil-ind> element of the application/vnd.3gpp.mcptt-info MIME 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 clause.

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

This clause 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 IWF shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [3] with the clarifications given below.

The IWF:

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: This is the case of a 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.

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

This clause 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", or the client homed in the IWF's imminent peril state of the group is set to "MIG 2: in-progress", the IWF performing the participating role:

1) shall include in the SIP INVITE request a Resource-Priority header field populated with the values for an MCPTT imminent peril group call as specified in clause 6.4.1.11.

NOTE: The IWF performing the participating role ideally would not need to maintain knowledge of the in-progress imminent peril state of the group (as tracked for the client by the 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 IWF performing the participating role determines that cancellation of the MCPTT imminent peril group call is authorized, or the MCPTT client imminent peril group state of the group is "MIG 1: no-imminent-peril" or "MIG 3: cancel-pending", the IWF performing the participating role:

1) shall include in the SIP INVITE request a Resource-Priority header field populated with the values for a normal MCPTT group call as specified in clause 6.4.1.11.

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

This clause 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 [26]; 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 IWF:

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

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

   a) if the MCPTT emergency alert state of the user homed in the IWF 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 of the user homed in the IWF 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 emergency group state of the user homed in the IWF of the group to "MEG 2: in-progress"; and

NOTE 1: This is the case of an IWF attempting to make an imminent peril group call when the group is in an in-progress emergency group state. The IWF will then receive a notification that the imminent peril call request was denied, however the IWF will be participating at the emergency level priority of the group.

NOTE 2: the emergency group state of the user homed in the IWF above is the view of the in-progress emergency state of the group for each user homed in the IWF.

4) if the SIP request for a priority group call sent by the IWF did not contain an <originated-by> element and if the MCPTT emergency alert state of the user homed in the IWF 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 of the user homed in the IWF 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 of the user homed in the IWF to "MEA 1: no-alert".

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

This clause is referenced from other procedures.

Upon the need to cancel an in-progress emergency group state of a group, the IWF performing the participating role shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [3] with the clarifications given below.

The IWF performing the participating role:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in 3GPP TS 24.379 [29], 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 emergency alert on the MCPTT group originated by a MCPTT user is to be cancelled:

   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 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.

6.4.1.11 Resource-Priority header field values

This clause is referenced from other procedures.

The IWF performing the participating role may populate the Resource-Priority header as described for the IWF performing the controlling role in clause 6.6.3.1.12.

6.4.2 MCPTT emergency private call conditions

6.4.2.1 SIP request for originating MCPTT emergency private calls

This clause is referenced from other procedures.

When the MCPTT emergency private call state is set to "MEPC 1: emergency-pc-capable", the IWF:

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 an MCPTT emergency alert is to be sent, 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 clause 6.5.1;

4) if the IWF has determined not to request 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".

6.4.2.2 Resource-Priority header field for MCPTT emergency private calls

This clause 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", or the MCPTT emergency private priority state of the call is set to "MEPP 2: in-progress", the IWF shall include in the SIP request a Resource-Priority header field populated with the values for an MCPTT emergency private call as specified in clause 6.4.1.11.

NOTE: The IWF 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 a request to cancel the MCPTT emergency private call and the MCPTT emergency private priority state of the private call is "MEPP 1: no-emergency" or "MEPP 3: cancel-pending", the IWF shall include in the SIP request a Resource-Priority header field populated with the values for a normal MCPTT private call as specified in clause 6.4.1.11.

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

This clause 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 IWF performing the participating role shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [3] with the clarifications given below.

The IWF performing the participating role:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in 3GPP TS 24.379 [29], 3GPP TS 24.379 [29], 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 1: This is the case where a private call is in emergency and the emergency is to be cancelled.

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 IWF decides that only the MCPTT emergency private call should be cancelled, the IWF performing the participating role:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in 3GPP TS 24.379 [29], 3GPP TS 24.379 [29], 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 2: This is the case where both an MCPTT emergency private call and an MCPTT emergency alert have been initiated and only the MCPTT emergency on the private call is to be cancelled. 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 IWF performing the participating role has indicated that the MCPTT emergency alert on the MCPTT private call should be cancelled in addition to the MCPTT emergency private call, the IWF performing the participating role:

1) shall include in the SIP re-INVITE request an application/vnd.3gpp.mcptt-info+xml MIME body as defined in 3GPP TS 24.379 [29], clause F.1 with the <emergency-ind> element set to "false";

2) shall:

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

4) shall clear the MCPTT emergency state.

NOTE 3: This is the case where both an MCPTT emergency private call and an MCPTT emergency alert have been initiated and both are to be cancelled.

6.5 Location information

6.5.1 Location information for location reporting

This procedure is initiated by the IWF performing the participating role when it is including location report information as part of a SIP request containing an MCPTT emergency alert.

NOTE 1: Location triggers are out of scope of the present document.

The IWF performing the participating role:

1) shall include an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in 3GPP TS 24.379 [29], clause F.3 with a <Report> element included in the <location-info> root element;

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

3) 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 3GPP TS 24.379 [29], clause F.3.3.

NOTE 2: According to local policy, additional location information elements specified in 3GPP TS 24.379 [29], clause F.3.3 can be included in the <CurrentLocation> element.

6.6 IWF server role procedures

6.6.1 Distinction of requests sent to the IWF

6.6.1.1 SIP INVITE request

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

- SIP INVITE requests routed to the IWF performing the participating role 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 [3] and the Request-URI contains a PSI of the IWF performing the terminating participating role. 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 IWF performing the controlling role as a result of PSI routing on the originating side in accordance with the originating procedures as specified in 3GPP TS 24.229 [3], or as a result of direct PSI routing, in accordance with the termination procedures as specified in 3GPP TS 24.229 [3], 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 [9]. 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 IWF performing the controlling role as a result of PSI routing on the originating side in accordance with the originating procedures as specified in 3GPP TS 24.229 [3], or as a result of direct PSI routing, in accordance with the termination procedures as specified in 3GPP TS 24.229 [3], 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 [9]. Such requests are known as "SIP INVITE request for controlling MCPTT function of an MCPTT group" in the procedures in the present document; and

- SIP INVITE requests routed to the IWF performing the non-controlling role of an MCPTT group as a result of direct PSI routing, in accordance with the termination procedures as specified in 3GPP TS 24.229 [3], 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 [9]; Such requests are known as "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" in the procedures in the present document.

6.6.1.2 SIP MESSAGE request

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

- SIP MESSAGE requests routed to the IWF performing the controlling role 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 "remotely-initiated-group-call-request". Such requests are known as "SIP MESSAGE request for remotely initiated group call request for controlling MCPTT function";

- SIP MESSAGE requests routed to the IWF performing the controlling role 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 "remotely-initiated-group-call-response". Such requests are known as "SIP MESSAGE request for remotely initiated group call response for controlling MCPTT function";

- SIP MESSAGE requests routed to the IWF performing the terminating participating role as a result of initial filter criteria with the Request-URI set to the public service identity of the IWF performing the terminating participating role 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 "remotely-initiated-group-call-request" or with the <response-type> element set to a value of "remotely-initiated-group-call-response". Such requests are known as "SIP MESSAGE request for remotely initiated group call for terminating participating MCPTT function";

- SIP MESSAGE requests routed to the IWF performing the terminating participating role with the Request-URI set to the public service identity of the IWF 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 request for emergency notification for terminating participating MCPTT function" in the procedures in the present document; and

- SIP MESSAGE requests routed to the IWF performing the controlling role with the Request-URI set to the public service identity of the IWF 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 request for emergency notification for controlling MCPTT function" in the procedures in the present document.

6.6.2 IWF participating role

6.6.2.1 Requests initiated by a participant homed in the IWF

6.6.2.1.1 SDP offer generation

6.6.2.1.1.1 On-demand session

This clause is referenced from other clauses.

The SDP offer generated by the IWF performing the participating role:

1) shall contain only one SDP media-level section for speech; and

2) shall contain an SDP media-level section for one media-floor control entity.

When composing the SDP offer according to 3GPP TS 24.229 [3], the IWF performing the participating role:

1) shall insert the IP address and port number selected by the IWF performing the participating role for the media stream in the SDP offer;

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

2) shall insert the IP address and port number selected by the IWF performing the participating role for the offered media floor control entity, if any, in the received SDP offer; and

3) shall include an "m=audio" media-level section for the 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 a call is being initiated to a group identity; and

      ii) if the IWF performing the participating role determines one or more preferred codecs;

      then the IWF:

      i) shall include the name of the chosen codec in the <encoding name> field of the "a=rtpmap" attribute as defined in IETF RFC 4566 [8];

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

4) if floor control shall be used during the session, shall include an "m=application" media-level section as specified in 3GPP TS 29.380 [31] 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 29.380 [31]; and

   b) the 'fmtp' attributes as specified in 3GPP TS 29.380 [31] clause 14;

5) if security between the IWF and the MCPTT system is required for a private call, 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 [22]; and

6) shall contain an "a=key-mgmt" attribute field with a "mikey" attribute value.

NOTE: End-to-end security of voice traffic is supported through the use of Interworking Security Data messages specified in 3GPP TS 29.582 [33]. Through the use of these messages, an LMR system can communicate security information to the LMR functionality of a device on the MCPTT system. This will allow the use of LMR algorithms and keys for encrypting and decrypting voice packets within the device that can be transmitted to and received from the LMR system.

6.6.2.1.2 Sending an INVITE request

This clause is referenced from other procedures.

When generating an initial SIP INVITE request according to 3GPP TS 24.229 [3] the IWF performing the participating role:

1) should include the Session-Expires header field according to IETF RFC 4028 [6]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

2) shall include the option tag "timer" in the Supported header field;

3) shall include in the P-Asserted-Identity header field the public service identity of the IWF performing the participating role;

4) shall include the g.3gpp.mcptt media feature tag into the Contact header; and

5) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [3]), into the P-Asserted-Service header field.

6.6.2.1.3 IWF sending a SIP BYE request

When the IWF is ending participation in an MCPTT session and decides to send a SIP BYE request, the IWF:

1) shall interact with the media plane as specified in clause 6.4 in 3GPP TS 29.380 [31];

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

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

4) shall set the P-Asserted-Identity header field of the outgoing SIP BYE request to the public service identity of the IWF;

5) may insert an application/vnd.3gpp.mcptt-info+xml MIME body into the outgoing SIP BYE request; and

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

Upon receiving a SIP 200 (OK) response to the SIP BYE request the IWF should complete any further actions necessary to dissociate the LMR user from the MCPTT session and shall interact with the media plane to release any resources as specified in clause 6.4 in 3GPP TS 29.380 [31] for releasing media plane resources associated with the SIP session with the controlling MCPTT function.

6.6.2.1.4 Priority call conditions

6.6.2.1.4.1 General

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

6.6.2.1.4.2 Determining authorisation for originating a priority group call

When the IWF performing the participating role needs to send a request to originate an MCPTT emergency group call and needs to determine if the request is an authorised request for an MCPTT emergency call, the IWF performing the participating role shall check the following:

1) if the IWF determines that the calling user is authorized for emergency-group-call; and

2) if the IWF determines that emergency-group-calls for the selected group are allowed;

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

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

NOTE 1: How the IWF authorizes a user to originate a priority group call is out of scope of the present document.

When the IWF performing the participating role needs to send a request 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 IWF performing the participating role shall check the following:

1) if the IWF determines that the calling user is authorized for imminent peril call; and

2) if the IWF determines that imminent paril calls for the selected group are allowed;

then the IWF performing the participating role shall consider the MCPTT imminent peril group call request to be an authorised request for an imminent peril group call;

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

NOTE 2: How the IWF authorizes a user to originate an imminent peril call is out of scope of the present document.

6.6.2.1.4.3 Determining authorisation for initiating or cancelling an MCPTT emergency alert

If the IWF performing the participating role needs to send a SIP request for an MCPTT emergency alert and:

1) if the calling user is authorized by the IWF to activate emergency alert; and

2) if the IWF allows emergency alert for the selected group;

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.

NOTE 1: How the IWF authorizes a user to originate a request for an MCPTT emergency alert is out of scope of the present document.

If the IWF performing the participating role needs to send a SIP request to cancel an MCPTT emergency alert to an MCPTT group, and if the calling user is authorized by the IWF to cancel an emergency alert, 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.

NOTE 2: How the IWF authorizes a user to cancel an MCPTT emergency alert is out of scope of the present document.

6.6.2.1.4.4 Validate priority request parameters

This clause is referenced from other procedures.

To validate the combinations of <emergency-ind>, <imminentperil-ind> and <alert-ind> which need to be sent in SIP requests, the IWF performing the participating role shall follow the procedures specified in 3GPP TS 24.379 [29], clause 6.3.3.1.17, with the IWF acting as the controlling function.

6.6.2.1.4.5 Retrieving Resource-Priority header field values

This clause is referenced from other procedures.

The IWF performing the participating role shall follow the procedures specified in clause 6.6.3.1.12 with the clarification that references in that procedure to the IWF performing the controlling role should be replaced with references to the IWF participating role.

6.6.2.1.5 Sending a SIP INVITE request on receipt of SIP 3xx response

This clause is referenced from other procedures.

Upon:

1) having sent a SIP INVITE request to the controlling MCPTT function; and
2) having received a SIP 302 (Moved Temporarily) response from the controlling MCPTT function sent to the SIP INVITE request in step 1) 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 IWF performing the participating role:

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 [5] included in the original SIP INVITE request sent to the controlling MCPTT function;
3) should include the Session-Expires header field according to IETF RFC 4028 [6]. 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 set the P-Asserted-Identity header field of the outgoing SIP INVITE request to the contents of the P-Asserted-Identity header field of the original SIP INVITE request sent to the controlling MCPTT function;
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 [3]), into the P-Asserted-Service header field of the outgoing SIP INVITE request;
9) shall copy the contents of the application/vnd.3gpp.mcptt-info+xml MIME body of the original SIP INVITE request sent to the controlling MCPTT function into the outgoing SIP INVITE request;
10) 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;
11) 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 by the IWF performing the participating role; and
12) 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.

6.6.2.2 Requests terminated to the IWF

6.6.2.2.1 SDP offer generation

The IWF performing the participating role shall follow the procedure in clause 6.6.2.1.1.

6.6.2.2.2 SIP BYE request towards the terminating IWF

6.6.2.2.2.1 On-demand

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

1) shall interact with the media plane as specified in clause 6.4 in 3GPP TS 29.380 [31] for releasing media plane resource associated with the SIP session; and
2) shall send a SIP 200 (OK) response to the SIP BYE request received from the controlling MCPTT function according to 3GPP TS 24.229 [3].

6.6.3 IWF controlling role

6.6.3.1 Requests initiated by the IWF performing the controlling role

6.6.3.1.1 Sending an INVITE request

This clause is referenced from other procedures.

The IWF performing the controlling role shall generate an initial SIP INVITE request according to 3GPP TS 24.229 [3].

The IWF performing the controlling role:

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 [9];
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 [5];
3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [3]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7] 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 [5];
5) shall include a Referred-By header field with the public service identity of the IWF;
6) should include the Session-Expires header field according to rules and procedures of IETF RFC 4028 [6]. The refresher parameter shall be omitted;
7) shall include the Supported header field set to "timer";
9) may include an unmodified Priv-Answer-Mode header field;
10) if the request will not contain a Priv-Answer-Mode header field, shall include an Answer-Mode header field; and
11) may include an application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing INVITE request.

6.6.3.1.2 Sending a SIP BYE request

When the IWF performing the controlling role needs to remove an MCPTT participant:

1) shall interact with the media plane as specified in 3GPP TS 29.380 [31] for the MCPTT session release;

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

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

If timer TNG3 (group call timer) has not expired, then when the last participant is removed from the MCPTT session, the IWF performing the controlling role shall stop timer TNG3 (group call timer).

When the MCPTT group session needs to be released, the IWF performing the controlling role shall send SIP BYE requests as described in this clause, to all MCPTT participants of the group session.

Upon receiving a SIP 200 (OK) response to a SIP BYE request the IWF performing the controlling role shall interact with the media plane as specified in clause 6.3 in 3GPP TS 29.380 [31] for releasing media plane resources associated with the session with the MCPTT clients.

6.6.3.1.3 Sending a SIP re-INVITE request for MCPTT emergency group call

This clause is referenced from other procedures.

The IWF performing the controlling role shall generate a SIP re-INVITE request according to 3GPP TS 24.229 [3].

The IWF performing the controlling role:

1) shall include an SDP offer with the media parameters as currently established with the terminating MCPTT client according to 3GPP TS 24.229 [3];

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 IWF performing the controlling role:

   a) shall include a Resource-Priority header field with the namespace populated with the values for an MCPTT emergency group call as specified in clause 6.6.3.1.12;

   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 received request included a request for an emergency alert and MCPTT emergency alerts are authorised for this group and MCPTT user as determined by the procedures of clause 6.6.3.1.8.1, shall populate the application/vnd.3gpp.mcptt-info+xml MIME body and application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in clause 6.6.3.1.7. 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 clause 6.6.3.1.12; 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 clause 6.6.3.1.8.4:

      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 3GPP TS 24.379 [29], clause 6.3.3.1.15 with the IWF acting as the controlling function, 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.

6.6.3.1.4 Sending a SIP INVITE request for MCPTT emergency group call

This clause is referenced from other procedures.

This clause 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 IWF performing the controlling role as the result of an action in clause 10.2.3.1.1.

The IWF performing the controlling role:

1) shall generate a SIP INVITE request as specified in clause 6.6.3.1.1;

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 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 IWF performing the controlling role;

5) shall include in the SIP INVITE request an SDP offer according to the procedures specified in 3GPP TS 24.379 [29], clause 6.3.3.1.1, with the IWF acting as the controlling function; and

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

   a) shall include a Resource-Priority header field populated with the values for an MCPTT emergency group call as specified in clause 6.6.3.1.12;

   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

      i) 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 clause 6.6.3.1.8.1, 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 clause 6.6.3.1.7. Otherwise, shall set the <alert-ind> element to a value of "false" in the application/vnd.3gpp.mcptt-info+xml MIME body; or

      ii) the call request originated from the IWF, and the IWF decides to indicate an emergency alert, 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 clause 6.6.3.1.7. Otherwise, shall set the <alert-ind> element to a value of "false" in the application/vnd.3gpp.mcptt-info+xml MIME body;

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 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 IWF performing the controlling role:

a) shall include a Resource-Priority header field populated with the values for an MCPTT imminent peril group call as specified in clause 6.6.3.1.12; 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".

6.6.3.1.5 Sending a SIP UPDATE request for Resource-Priority header field correction

This clause is referenced from other procedures.

This clause 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 IWF performing the controlling role 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 [3] with the clarifications provided specified in 3GPP TS 24.379 [29], clause 6.3.3.2.3.1, with the IWF acting as the controlling function;

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 3GPP TS 24.379 [29], clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function; and

4) shall send the SIP 183 (Session Progress) response towards the MCPTT client according to 3GPP TS 24.229 [3].

Upon receiving a SIP PRACK request to the SIP 183 (Session Progress) response the IWF performing the controlling role:

1) shall send the SIP 200 (OK) response to the SIP PRACK request according to 3GPP TS 24.229 [3].

2) shall generate a SIP UPDATE request according to 3GPP TS 24.229 [3] 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 3GPP TS 24.379 [29], clause 6.3.3.1.1, with the IWF acting as the controlling function;

4) if the in-progress emergency group state of the group is set to a value of "true" the IWF performing the controlling role shall include a Resource-Priority header field populated for an MCPTT emergency group call as specified in clause 6.6.3.1.12; 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 IWF performing the controlling role:

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 clause 6.6.3.1.12; 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 clause 6.6.3.1.12.

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.

6.6.3.1.6 Generating a SIP re-INVITE request to cancel an in-progress emergency

This clause is referenced from other procedures.

This clause describes the procedures for generating a SIP re-INVITE request to cancel the in-progress emergency state of a group. The procedure is initiated by the IWF performing the controlling role when it determines the cancellation of the in-progress emergency state of a group is required.

The IWF performing the controlling role:

1) shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [3] with the clarifications specified in 3GPP TS 24.379 [29] clause 6.3.3.1.9, with the IWF acting as the controlling function;

2) shall include a Resource-Priority header field populated with the values for a normal MCPTT group call as specified in clause 6.6.3.1.12; and

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

6.6.3.1.7 Populate mcptt-info and location-info MIME bodies for emergency alert

This clause is referenced from other procedures.

This clause 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 IWF performing the controlling role when it has received request initiating an MCPTT emergency alert and generates a message containing the MCPTT emergency alert information required by 3GPP TS 23.379 [2].

The IWF performing the controlling role:

1) shall include, if not already present, an application/vnd.3gpp.mcptt-info+xml MIME body as specified in 3GPP TS 24.379 [29], clause F.1, and set the <alert-ind> element to a value of "true";

2) shall determine the value of the user's Mission Critical Organization identity.

NOTE: How the IWF determines the user's Mission Critical Organization identity is out of scope of the present document;

3) shall include in the <mcpttinfo> element containing the <mcptt-Params> element containing an <mc-org> element set to the value of the user's Mission Critical Organization identity; and

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

6.6.3.1.8 Authorisations

6.6.3.1.8.1 Determining authorisation for initiating an MCPTT emergency alert

If the IWF performing the controlling role 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 IWF performing the controlling role shall check the following conditions:

1) if the user is authorized by the IWF to initiate an emergency alert; and

2) if the IWF allows emergency alerts on the group;

then the MCPTT emergency alert request shall be considered to be an authorised request for an MCPTT emergency alert targeted to an 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.

NOTE 1: How the IWF authorizes a user to initiate alerts and how the IWF decides to allow emergency alerts on a group is out of scope of the present document.

If the IWF performing the controlling role has received a SIP request targeted to a user with the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body set to a value of "true", the IWF performing the controlling role shall check the following condition:

1) if the calling user is authorized by the IWF for emergency alerts;

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

NOTE 2: How the IWF authorizes a user to initiate alerts to other users is out of scope of the present document.

Editor's note: How and whether the IWF obtains user profile information for MCPTT users, and whether the MCPTT system needs access to IWF user profile information is FFS.

6.6.3.1.8.2 Determining authorisation for initiating an MCPTT emergency group or private call

If the IWF performing the controlling role 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 MCPTT user is authorized by the IWF to initiate emergency calls and if the group is configured to allow emergency calls, then the IWF performing the controlling role shall consider the MCPTT emergency group call request to be an authorised request for an MCPTT emergency group call and skip the remaining step; or

NOTE 1: How the IWF determines whether the user is authorized to initiate an emergency group call and whether the group supports emergency calls is out of scope of the current document.

2) if the IWF performing the controlling role 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 IWF performing the controlling role shall consider the MCPTT emergency group call request to be an unauthorised request for an MCPTT emergency group call.

If the IWF performing the controlling role 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", the IWF performing the controlling role determines whether the user is authorized to initiate an emergency private call.

NOTE 2: How the IWF determines whether the user is authorized to initiate an emergency private call is out of scope of the current document.

Editor's note: How and whether the IWF obtains user profile information for MCPTT users, and whether the MCPTT system needs access to IWF user profile information is FFS.

6.6.3.1.8.3 Determining authorisation for cancelling an MCPTT emergency alert

If the IWF performing the controlling role 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", the IWF may authorize the MCPTT emergency alert cancellation.

NOTE: How the IWF determines whether to authorize a user to cancel an emergency alert is out of scope of the present document.

6.6.3.1.8.4 Determining authorisation for cancelling an MCPTT emergency group or private call

If the IWF performing the controlling role 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", the IWF may authorize the MCPTT emergency group call cancellation request.

NOTE 1: How the IWF determines whether to authorize a user to cancel a group call emergency is out of scope of the present document.

If the IWF performing the controlling role 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", the IWF may authorize the MCPTT emergency private call cancellation request.

NOTE 2: How the IWF determines whether to authorize a user to cancel a private call emergency is out of scope of the present document.

6.6.3.1.8.5 Determining authorisation for initiating an MCPTT imminent peril call

If the IWF performing the controlling role 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 MCPTT user is authorized by the IWF performing the controlling role to initiate an imminent peril call; and

2) if the IWF allows the group to support imminent peril calls;

NOTE: How the IWF authorizes the user to initiate imminent peril calls and how the IWF determines whether to allow imminent peril calls on a group is out of scope of the present document.

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.

Editor's note: How and whether the IWF obtains user profile information for MCPTT users, and whether the MCPTT system needs access to IWF user profile information is FFS.

6.6.3.1.8.6 Determining authorisation for cancelling an MCPTT imminent peril call

If the IWF performing the controlling role 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", the IWF may authorize the MCPTT imminent peril call cancellation request.

NOTE: How the IWF determines whether to authorize a user to cancel an imminent peril call is out of scope of the present document.

6.6.3.1.8.7 Sending a SIP OPTIONS request to authorise an MCPTT user at a non-controlling MCPTT function of a MCPTT group

This clause is referenced from other procedures.

The IWF performing the controlling role:

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 [3] and the IETF RFC 3261 [14] 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 IWF performing the controlling role 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 [3]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7];

   c) shall include in the P-Asserted-Identity header field, the public service identity of the IWF performing the controlling role;

   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 [3]; 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 not homed in the IWF performing the controlling role generate a SIP OPTIONS request according to 3GPP TS 24.229 [3] and IETF RFC 3261 [14] 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 of the constituent group;

NOTE 2: How the IWF performing the controlling role 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 [3]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7];

c) shall include in the P-Asserted-Identity header field, the public service identity of the IWF performing the controlling role;

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 of the constituent group; 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 [3].

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 3GPP TS 24.379 [29] clause 4.4, the IWF acting as the controlling 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 application/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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the controlling 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server, and if more than one OPTIONS request were sent and if no other responses to the SIP OPTIONS request are expected, the IWF performing the controlling role:

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 IWF performing the controlling role:

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 Found) 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.

6.6.3.1.9 Generating a SIP 403 response for priority call request rejection

If the IWF performing the controlling role 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 clause 6.6.3.1.8.2, 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 3GPP TS 24.379 [29], clause F.1 with the <mcpttinfo> element containing the <mcptt-Params> element with the <emergency-ind>.

6.6.3.1.10 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 IWF performing the controlling role:

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 clause 6.6.3.1.6; and

   b) send the SIP re-INVITE request towards the MCPTT client according to 3GPP TS 24.229 [3]; and

3) shall for each affiliated but non-participating member of the group:

   a) generate a SIP MESSAGE request according to 3GPP TS 24.379 [29] clause 6.3.3.1.11, with the IWF acting as the controlling function 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 [3]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7]; and

d) send the SIP MESSAGE request towards the MCPTT client according to rules and procedures of 3GPP TS 24.229 [3].

Upon receiving a SIP 200 (OK) response to a re-SIP INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31].

6.6.3.1.11 Sending a SIP INFO request in the dialog of a SIP request for a priority call

This clause is referenced from other procedures and describes how the IWF performing the controlling role generates a SIP INFO request due to the receipt of a SIP request for a priority call.

The IWF performing the controlling role:

1) shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [3] and IETF RFC 6086 [26];

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 clause 6.6.3.1.8.1, 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 [3].

6.6.3.1.12 Retrieving Resource-Priority header field values

This clause is referenced from other procedures.

The IWF performing the controlling role may populate the Resource-Priority header field to assist interworked MC systems in setting bearer priorities. The IWF can set emergency, imminent peril and normal priorities for private and group calls. The priority values and namespaces are as specified in IETF RFC 8101 [23].

NOTE: How the IWF obtains the values for Resource-Priority header fields is out of scope of the present document.

6.6.3.2 Requests terminated by the IWF performing the controlling role

6.6.3.2.1 Receiving a SIP BYE request

Upon receiving a SIP BYE request the IWF performing the controlling role:

1) shall interact with the media plane as specified in clause 6.3 in 3GPP TS 29.380 [31] for releasing the media plane resource associated with the SIP session towards the MCPTT client;

NOTE: The IWF performing the non-controlling role 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 [3];

3) shall check the MCPTT session release policy as specified in clause 6.6.7.1 and clause 6.6.7.2 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 clause 6.6.3.1.2 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:

   a) 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 3GPP TS 24.379 [29], clause 10.1.3.4.2 with the IWF acting as the controlling MCPTT function.

Upon receiving a SIP 200 (OK) response to the SIP BYE request the IWF performing the controlling shall interact with the media plane as specified in clause 6.3 in 3GPP TS 29.380 [31] for releasing media plane resources associated with the SIP session with the MCPTT participant.

6.6.3.3 Handling of the acknowledged call setup timer (TNG1)

When the IWF performing the controlling role receives a SIP INVITE request to initiate a group session and there are members of the group that are affiliated and are deemed by the IWF to be required for the call, then the IWF performing the controlling role shall start timer TNG1 (acknowledged call setup timer), prior to sending out SIP INVITE requests inviting group members to the group session.

NOTE 1: How the IWF obtains the value of the TNG1 timer is out of scope of the present document.

NOTE 2: How the IWF determines the required participants for the call, whether to require certain participants for the call or whether to require a certain number of participants for the call is out of scope of the present document.

When the IWF performing the controlling role receives all SIP 200 (OK) responses to the SIP INVITE requests, from all affiliated and required members then the IWF performing the controlling role 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 required number of participants, the IWF performing the controlling role shall send a SIP 200 (OK) response to the initiating MCPTT client and shall interact with the media plane as specified in 3GPP TS 29.380 [31].

NOTE 3: MCPTT clients that are affiliated but are not required members that have not yet responded will be considered as joining an ongoing session when the IWF performing the controlling role 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 required by the IWF performing the controlling role, then the IWF performing the controlling role 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 number required by the IWF performing the controlling role, before continuing with the timer TNG1 expiry procedures in this clause.

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 number required by the IWF performing the controlling role, the IWF performing the controlling role shall execute the steps described below:

1) if the IWF is configured to "proceed" with the setup of the group call, then the IWF performing the controlling role:

   a) shall perform the following actions:

i) generate a SIP 200 (OK) response to the SIP INVITE request as specified in the 3GPP TS 24.379 [29] clause 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server MCPTT function;

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 3GPP TS 24.379 [29] clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

iv) interact with the media plane as specified in 3GPP TS 29.380 [31]; and

NOTE 4: 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 [3];

b) when a SIP 200 (OK) response to a SIP INVITE request is received from an invited MCPTT client the IWF performing the controlling role 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 IWF performing the controlling role receives a SIP BYE request from an invited MCPTT client, shall take the actions specified in clause 6.6.3.2.1 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 clause 6.6.3.4 and send a SIP NOTIFY request according to 3GPP TS 24.229 [3] to the MCPTT clients which have subscribed to the conference event package; and

2) if the IWF is configured to "abandon" the setup of the group call, then the IWF performing the controlling role 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

b) for each confirmed dialog at the IWF performing the controlling role, send a SIP BYE request towards the MCPTT clients invited to the group session in accordance with 3GPP TS 24.229 [3] and interact with the media plane as specified in 3GPP TS 29.380 [31]; and

c) for each non-confirmed dialog at the IWF performing the controlling role, send a SIP CANCEL request towards the MCPTT clients invited to the group session in accordance with 3GPP TS 24.229 [3].

If the IWF performing the controlling role receives a final SIP 4xx, 5xx or 6xx response from an affiliated and required group member prior to expiry of timer TNG1 (acknowledged call setup timer) and based on policy, the IWF performing the controlling role decides not to continue with the establishment of the group call without the affiliated and required group member, then the IWF performing the controlling role:

NOTE 5: 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server.

If:

1) the IWF performing the controlling role receives a final SIP 4xx, 5xx or 6xx response from an affiliated and 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 required number of participants; and

3) based on policy, the IWF performing the controlling role decides to continue with the establishment of the group call without the affiliated and required group member;

then the IWF performing the controlling role:

NOTE 6: 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 3GPP TS 24.379 [29] clause 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

   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 3GPP TS 24.379 [29] clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

   e) interact with the media plane as specified in 3GPP TS 29.380 [31]; and

NOTE 7: 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 [3].

6.6.3.4 Generating a SIP NOTIFY request

The IWF performing the controlling role shall generate a SIP NOTIFY request according to 3GPP TS 24.229 [3] with the clarification in this clause.

In the SIP NOTIFY request, the IWF performing the controlling role:

1) shall set the P-Asserted-Identity header field to the public service identity of the IWF performing the controlling role;

2) shall include an Event header field set to "conference";

3) shall include an Expires header field set to 3600 seconds according to IETF RFC 4575 [15], 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 [3]), in a P-Preferred-Service header field according to IETF RFC 6050 [7]; 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 IWF performing the controlling role shall include an application/conference-info+xml MIME body according to IETF RFC 4575 [15] with the following limitations:

1) the IWF performing the controlling role shall include the MCPTT group ID of the MCPTT group in the "entity" attribute of the <conference-info> element;

2) for each non-IWF connected participant in the MCPTT session with the exception of non-controlling MCPTT functions, the IWF performing the controlling role shall include a <user> element. The <user> element:

NOTE 1: Non-controlling MCPTT functions will appear as a participant in temporary group sessions.

a) shall 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 user that originated the 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 IETF RFC 4575 [14]; and

c) may include the <roles> element.

NOTE 2: The usage of <roles> is only applicable for human consumption.

6.6.3.5 Handling of the group call timer (TNG3)

6.6.3.5.1 General

When the IWF performing the controlling role receives a SIP INVITE request to initiate a group session, then after an MCPTT session identity has been allocated for the group session, the IWF performing the controlling role shall start timer TNG3 (group call timer).

NOTE 1: How the IWF determines the value of the TNG3 timer is out of scope of the present document.

If the IWF does not have a TNG3 timer value, then the IWF performing the controlling role shall not start timer TNG3 (group call timer).

NOTE 2: The group call timer 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, if the IWF is hosting at least one of the active group calls shall stop timer TNG3 (group call timer) for each hosted group call, and the IWF performing the controlling role hosting the temporary group call shall start timer TNG3 (group call timer) for the temporary group call.

NOTE 3: MCPTT server(s) other than the IWF that are 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 IWF performing the controlling role 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 IWF performing the controlling role shall stop timer TNG3 (group call timer).

On expiry of timer TNG3 (group call timer), the IWF performing the controlling role shall release the MCPTT session by following the procedures in clause 6.6.3.1.2;

6.6.3.5.2 Interaction with the in-progress emergency group call timer (TNG2)

If the IWF performing the controlling role 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 IWF performing the controlling role shall stop timer TNG3 (group call timer) and shall start timer TNG2 (in-progress emergency group call timer). If timer TNG2 (in-progress emergency group call timer) is running and the

MCPTT emergency group call is cancelled, then the IWF performing the controlling role shall stop timer TNG2 (in-progress emergency group call timer) and shall start timer TNG3 (group call timer).

NOTE 1: How the IWF determines the value of the TNG2 and TNG3 timers is out of scope of the present document.

If timer TNG2 (in-progress emergency group call timer) is running and sequentially expires, then the controlling MCPTT function shall start timer TNG3 (group call timer).

NOTE 2: 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.

6.6.4 IWF non-controlling role

6.6.4.1 Request initiated by the IWF performing the non-controlling role of a group

6.6.4.1.1 SDP offer generation

The SDP offer is generated based on the received SDP offer to be sent to MCPTT clients that are a member of the group homed in the IWF. The SDP offer generated by the IWF performing the non-controlling role of a group:

1) shall include only one SDP media-level section for 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 [3], the IWF performing the non-controlling role of a 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 IWF performing the non-controlling role;

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 IWF performing the non-controlling role; and

4) shall include the offered media floor control entity 'fmtp' attributes as specified in 3GPP TS 29.380 [31] clause 14.

6.6.4.1.2 Sending an INVITE request towards the MCPTT client

This clause is referenced from other procedures.

This clause covers the situation where a group homed in the IWF is a constituent group of a group homed in an MCPTT system.

If the IWF receives a "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" and does not support group regroup procedures, the IWF shall reject the SIP INVITE request with a SIP 403 (Forbidden) response with the warning text set to "100 function not allowed due to local policy" in a Warning header field as specified in 3GPP TS 24.379 [29] clause 4.4, and shall not execute the remainder of this procedure.

If there are MCPTT clients that are members of the group, the IWF performing the non-controlling role of a group shall generate initial SIP INVITE requests according to 3GPP TS 24.229 [3].

NOTE 1: How the IWF includes participants homed in the IWF is out of scope.

For each SIP INVITE request, the IWF performing the non-controlling role of a 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 [9];

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 [5];

3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [3]), in a P-Asserted-Service-Id header field according to IETF RFC 6050 [7] 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 [5];

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 2: How the IWF finds the address of the terminating participating MCPTT 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 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 IWF in the P-Asserted-Identity header field;

9) shall include the received Referred-By header field with the public service identity of the IWF;

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

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

12) shall include an unmodified Answer-Mode header field, if present in the incoming SIP INVITE request; and

13) shall include the warning text set to "148 MCPTT group is regrouped" in a Warning header field as specified in 3GPP TS 24.379 [29] clause 4.4.

NOTE 4: 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 29.380 [31].

6.6.4.1.3 Sending a SIP INFO request

This clause is referenced from other procedures.

This clause covers the situation where a group homed in the IWF is a constituent group of a group homed in an MCPTT system.

If the IWF performing the non-controlling role receives a "SIP INVITE request for non-controlling MCPTT function of an MCPTT group" and does not support group regroup procedures, the IWF shall reject the SIP INVITE request with a SIP 403 (Forbidden) response with the warning text set to "100 function not allowed due to local policy" in a Warning header field as specified in 3GPP TS 24.379 [29] clause 4.4, and shall not execute the remainder of this procedure.

The IWF shall generate a SIP INFO request according to rules and procedures of 3GPP TS 24.229 [3] and IETF RFC 6086 [26].

The IWF:

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;

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 3GPP TS 24.379 [29] clause F.5.3;

   b) the SSRC of the MCPTT client or participant homed in the IWF 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 or participant homed in the IWF 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 29.380 [31] clause 8.2.3.13; and

   h) if available, additional information in the <floor-indicator> element; and

4) if:

   a) the user with permission to send media is an MCPTT client, and if:

      i) the IWF has location information (see 3GPP TS 24.379 [29] clause 13.2.4) for the MCPTT client;

      ii) the location information for the MCPTT client either has not been sent to the controlling MCPTT function or has changed since last sent to the MCPTT controlling function; and

      iii) the IWF determines that the location of the MCPTT client is allowed to be sent when the MCPTT user is talking; or

   b) the user with permission to send media is a participant homed in the IWF, and if:

      i) location information for the user with permission to send media homed in the IWF is available;

      ii) the location information for the participant homed in the IWF has either not been sent to the controlling MCPTT function or has changed since last sent to the controlling MCPTT function; and

      iii) the IWF determines that the location of the participant homed in the IWF is allowed to be sent when the participant homed in the IWF is talking;

   then shall include an application/vnd.3gpp.mcptt-location-info+xml MIME body with a <Report> element included in the <location-info> root element.

6.6.4.1.4 Sending an INVITE request towards the controlling MCPTT function

This clause is referenced from other procedures.

The IWF shall generate a SIP INVITE request according to rules and procedures of 3GPP TS 24.229 [3].

The IWF:

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 [9];

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

3) shall set the Request-URI to the public service identity of the controlling MCPTT function;

4) shall include an application/vnd.3gpp.mcptt-info+xml MIME body with:

a) the <mcptt-request-uri> element set to the group identity;

b) the <mcptt-calling-user-id> element set to the MCPTT ID of the calling user; and

c) 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 [16];

5) shall include the public service identity of the IWF in the P-Asserted-Identity header field;

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

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

6.6.4.2 Requests terminated by the non-controlling MCPTT function of an MCPTT group

6.6.4.2.1 SDP answer generation

When composing the SDP answer according to 3GPP TS 24.229 [3], the IWF performing the non-controlling role of a 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 IWF performing the non-controlling role; 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 IWF performing the non-controlling role; and

   b) shall include 'fmtp' attributes as specified in 3GPP TS 29.380 [31] clause 14.

6.6.4.2.2 Sending a SIP response to the SIP INVITE request

6.6.4.2.2.1 Sending a SIP 183 (Session Progress) response

When sending a SIP 183 (Session Progress) the IWF performing the non-controlling role of a group:

1) shall generate a SIP 183 (Session Progress) response according to 3GPP TS 24.229 [3];

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 determined by the IWF performing the non-controlling role 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 [13].

6.6.4.2.2.2 Sending a SIP 200 (OK) response

When sending a SIP 200 (OK) response, the IWF performing the non-controlling role of a group homed in the IWF:

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

2) shall include the Session-Expires header field and start supervising the SIP session according to rules and procedures of IETF RFC 4028 [6], "UAS Behaviour". 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 IWF performing the non-controlling role 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 from MCPTT clients 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 [13]; 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.

6.6.4.3 Generating a SIP NOTIFY request

The IWF performing the non-controlling role shall generate a SIP NOTIFY request according to 3GPP TS 24.229 [3] with the clarification in this clause.

In the SIP NOTIFY request, the IWF:

1) shall set the P-Asserted-Identity header field to the public service identity of the IWF;

2) shall include an Event header field set to "conference";

3) shall include an Expires header field set to 3600 seconds according to IETF RFC 4575 [15], 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 [3]), in a P-Preferred-Service header field according to IETF RFC 6050 [7]; 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 IWF shall include application/conference-info+xml MIME body according to IETF RFC 4575 [15] as specified in clause 6.6.3.4 with the following exceptions:

1) the IWF performing the non-controlling role 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 IWF shall include stored conference status information received in SIP NOTIFY requests from the controlling MCPTT function in 3GPP TS 24.379 [29] clause 10.1.3.5.3 and status information about MCPTT participants that are members of the group.

6.6.5 Retrieving and processing a group document

6.6.5.1 General

How an IWF performing the controlling role of a group or performing the non-controlling role of a group obtains information about the group is out of scope of the present document.

NOTE: During the group regrouping operation as specified in 3GPP TS 24.481 [16], the IWF performing the controlling role is notified of the constituent MCPTT group identities associated with the TGI.

6.6.5.2 Rules for joining a group session

The following conditions shall be met for the IWF performing the controlling role to allow an MCPTT user to join an existing group session:

1) the MCPTT user is a member of the group; and

2) the MCPTT user is authorized to join the group;

If both of the above conditions are met, then the MCPTT user shall be authorised to join the group session.

6.6.5.3 Determining the group members to invite

The IWF shall only invite affiliated group members to a group session. The IWF determines whether MCPTT users are affiliated members of its group by following the procedures specified in 3GPP TS 24.379 [29], clause 6.3.6.

NOTE 1: The term "affiliated group members" used above also includes those members that are implicitly affiliated by the IWF performing the controlling role.

NOTE 2: The IWF need not store its group parameters in a GMS as described in 3GPP TS 24.481 [16] the IWF will have to respond to queries from other systems on its IWF-3 interface, which is based upon the CSC-16 interface described in 3GPP TS 23.283 [28].

The IWF may limit the maximum number of participants.

6.6.6 Error handling

6.6.6.1 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 IWF, the IWF performing the participating role or the controlling role shall return a SIP 404 (Not Found) response.

6.6.7 Session release policy

6.6.7.1 Session release policy for group call

If:

1) the call is a pre-arranged group call and if the IWF performing the controlling role receives an indication from the media plane that the T4 (Inactivity) timer specified in 3GPP TS 29.380 [31] expired and if there is at least one participant of the prearranged group call that is an MCPTT user;

2) there are only one or no participants in the call, including both MCPTT participants and participants homed in the IWF;

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 call;

4) less than the minimum number of affiliated group members is present;

5) timer TNG3 (group call timer) expires; or

6) the call is a broadcast group call and if the controlling MCPTT function receives an indication from the media plane that the T4 (Inactivity) timer specified in 3GPP TS 29.380 [31] expired;

then the IWF performing the controlling role;

1) shall release the MCPTT session for the group call if any participants are MCPTT users.

6.6.7.2 Session release policy for private call

If:

1) IWF performing the controlling role decides that a private call has been inactive for longer than a locally determined period; or

2) there are only one or no participants in the MCPTT session;

the IWF performing the controlling role shall release the MCPTT session for a private call.

6.7 Implicit floor request

A SIP re-INVITE request fulfilling the following criteria shall be regarded by the IWF performing the controlling role as an implicit floor request when the originator of the request:

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 29.380 [31] clause 12.

In all other cases the SIP (re-)INVITE request shall be regarded as received without an implicit floor request.

6.8 Confidentiality and Integrity Protection

6.8.1 General

6.8.1.1 Applicability and exclusions

The procedures in clause 6.8 apply in general to all procedures described in clause 9, clause 10, clause 11 and clause 12.

6.8.1.2 Performing XML content encryption

Whenever the IWF includes XML elements or attributes pertaining to the data specified in 3GPP TS 24.379 [29] clause 4.8 in SIP requests or SIP responses, the IWF shall perform the procedures in clause 6.8.2.1.1, with the exception that when the IWF 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 IWF shall perform the procedures specified in clause 6.8.2.2.

NOTE: The procedure in clause 6.8.2.1.1 first determines (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.

6.8.1.3 Performing integrity protection on an XML body

The IWF shall perform the procedures in clause 6.8.3.2 just prior to sending a SIP request or SIP response.

NOTE: The procedure in clause 6.8.3.2 first determines 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.

6.8.1.4 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 an SPK as specified in 3GPP TS 24.379 [29] clause 4.8. An XPK-ID (SPK-ID) is used to key the XPK (SPK). It is assumed that before the procedures in this clause are called, the SPK/SPK-ID is available on the sender and recipient of the encrypted content as described in 3GPP TS 24.379 [29] clause 4.8.

The procedures in 3GPP TS 24.379 [29], clause 6.6.2.3 and 3GPP TS 24.379 [29] clause 6.6.2.4 are used with an 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 [27]:

1) IWF sends confidentiality protected content to an MCPTT server in the same domain; and

2) IWF sends confidentiality protected content to an MCPTT server in another domain.

6.8.2 Confidentiality Protection

6.8.2.1 Procedures for sending confidentiality protected content

6.8.2.1.1 IWF performing any role of an MCPTT server

If the IWF performing any role of an MCPTT server determines locally that it needs to confidentiality protect content sent to an MCPTT server, then sending confidentiality protected content between MCPTT servers is enabled.

When sending confidentiality protected content, the IWF:

1) shall use the appropriate keying information specified in clause 6.8.1.4;

2) shall perform the procedures in 3GPP TS 24.379 [29] clause 6.6.2.3.3 to confidentiality protect XML elements containing the content described in 3GPP TS 24.379 [29] clause 4.8; and

3) shall perform the procedures in 3GPP TS 24.379 [29] clause 6.6.2.3.4 to confidentiality protect URIs in XML attributes for URIs described in 3GPP TS 24.379 [29] clause 4.8.

If the IWF determines locally that it does not need to confidentiality protect content sent to an MCPTT server, then sending confidentiality protected content between MCPTT servers is disabled, and content is included in XML elements and attributes without encryption.

6.8.2.2 IWF copying received XML content

The following procedure is executed when an IWF 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 IWF:

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 3GPP TS 24.379 [29] clause 6.6.2.4.1:

   a) shall use the keying information described in clause 6.8.1.4 to decrypt the content within the XML element by following the procedures specified in 3GPP TS 24.379 [29] clause 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 clause 6.8.2.1.1, then for each decrypted XML element:

i) shall re-encrypt the content within the XML element using the keying information described in clause 6.8.1.4 and by following the procedures specified in 3GPP TS 24.379 [29] clause 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 clause 6.8.2.1.1, 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 3GPP TS 24.379 [29] clause 6.6.2.4.1:

a) shall use the keying information described in clause 6.8.1.4 to decrypt the URI value of the XML attribute by following the procedures specified in 3GPP TS 24.379 [29] clause 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 clause 6.8.2.1.1, then for each decrypted XML element:

i) shall re-encrypt the URI value of the XML attribute using the keying information described in clause 6.8.1.4 and by following the procedures specified in 3GPP TS 24.379 [29] clause 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 clause 6.8.2.1.1, shall include the decrypted value in the same XML MIME body of the outgoing SIP request.

6.8.3 Integrity Protection of XML documents

6.8.3.1 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 an SPK as specified in 3GPP TS 24.379 [29] clause 4.8. An XPK-ID (SPK-ID) is used to key the XPK (SPK). It is assumed that before the procedures in 3GPP TS 24.379 [29] clause 6.6.3.3 and 3GPP TS 24.379 [29] clause 6.6.3.4 are called, the SPK/SPK-ID are available on the sender and recipient of the integrity protected content, as described in 3GPP TS 24.379 [29] clause 4.8.

The procedures in 3GPP TS 24.379 [29] clause 6.6.3.3 and 3GPP TS 24.379 [29] clause 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 [27]:

1) IWF sends integrity protected content to an MCPTT server in the same domain; and

2) IWF sends integrity protected content to an MCPTT server in another domain.

6.8.3.2 Integrity protection at the IWF

The IWF determines locally whether sending integrity protected content from the IWF to an MCPTT server is enabled.

NOTE 1: How the IWF determines whether to integrity protect content is out of scope of the present document.

When sending integrity protected content, the IWF shall use the appropriate keying information specified in clause 6.8.3.1 and shall perform the procedures in 3GPP TS 24.379 [29] clause 6.6.3.3.3 to integrity protect XML MIME bodies.

NOTE 2: Each XML MIME body is integrity protected separately.

6.9 Priority sharing

The IWF performing the participating role shall enable or disable priority sharing as specified in 3GPP TS 24.229 [3].

6.10 Private call parameters

6.10.1 Private call parameter check

Parameters of an incoming SIP INVITE are indicated as follows:

1) floor control. Floor control operation is indicated by an SDP offer with a media-level section for a media-floor control entity;

2) commencement mode. The requested commencement mode is according to the Answer-mode header, i.e. either "auto" or "manual"; and

3) implicit floor request. An implicit floor request is indicated by inclusion of the "mc_implicit_request" 'fmtp' attribute for the floor control in the SDP offer/answer as specified in 3GPP TS 29.380 [31] clause 12.

Additional LMR specific parameters, such as LMR encryption mode, are out of scope of the present document. The LMR specific parameters may be conveyed in the <LMR-specific-params> element of the <private-call-params> element of the <anyExt> element of the MIME body <mcpttinfo> root element as defined in 3GPP TS 24.379 [29], clause F.1.

6.10.2 Private call parameter response values

To reject a private call due to unsupported parameters, the IWF performing the participating role shall include in its response to the SIP INVITE a list of parameters from the incoming SIP INVITE that it does support.

To indicate support for one or more private call parameters, in the <private-call-params> element of the <anyExt> element of the <mcpttinfo> root element in the XML body, the IWF:

1) if floor control is requested in the incoming SIP INVITE and is supported, shall include the <floor-control> element;

2) if "without" floor control is requested in the incoming SIP INVITE and is supported by the IWF (i.e. full duplex is not supported), shall include the <without-floor-control> element;

3) if implicit floor is requested in the incoming SIP INVITE and is supported by the IWF (i.e. the IWF need not talk first), shall include the <implicit-floor> element;

4) if floor is not implicitly requested in the incoming SIP INVITE and the IWF supports floor not being implicitly requested (i.e. the IWF must talk first), shall include the <without-implicit-floor> element;

5) if manual commencement is requested in the incoming SIP INVITE and is supported by the IWF, shall include the <manual-commencement> element; and

6) if automatic commencement is requested in the incoming SIP INVITE and is supported by the IWF, shall include the <automatic-commencement> element.

7 Registration and service authorisation

The present document does not specify any registration or service authorization procedures for users homed in the IWF.

8 Pre-established session

The present document does not specify any pre-established session procedures for users homed in the IWF.

9 Affiliation

9.1 General

Clause 9.2.1.2 contains the procedures for explicit and implicit affiliation of a user homed in the IWF at the IWF homing that user.

Clauses in 9.2.1.2 also cover the case where the IWF manages affiliation to a group on behalf of the users homed in that IWF (i.e. having only one affiliation for a whole set of users homed in the IWF). In that case, the IWF needs to implement the same set of procedures but in those procedures, it shall use the MCPTT ID and the MCPTT client ID that are associated with the IWF itself instead of the ones associated with a user homed in the IWF.

NOTE: How the MCPTT ID and MCPTT client ID associated with the IWF are determined is out of the scope of this specification.

Clause 9.2.1.3 contains the procedures for explicit and implicit affiliation of an MCPTT user at the IWF owning the MCPTT group.

The procedures for implicit affiliation in this clause are triggered at the IWF for a user homed in the IWF in the following circumstances:

- when the IWF performing the participating role attempts to join an MCPTT chat group for a user homed in the IWF that is not already affiliated to the MCPTT group;
- when the IWF performing the participating role attempts to initiate an MCPTT emergency group call or MCPTT imminent peril group call for a user homed in the IWF that is not already affiliated to the MCPTT group;
- when the IWF performing the participating role attempts to initiate an MCPTT emergency alert targeted to an MCPTT group for a user homed in the IWF that is not already affiliated to the MCPTT group.

The procedures for implicit affiliation in this clause are triggered at the IWF owning the MCPTT group in the following circumstances:

- on receipt of a SIP INVITE request from an MCPTT server serving an MCPTT user where the MCPTT user wants to join an MCPTT chat group homed in the IWF and the MCPTT client is not already affiliated to the MCPTT group homed in the IWF;
- on receipt of a SIP INVITE request from an MCPTT server serving an MCPTT user where the MCPTT user initiates an MCPTT emergency group call or MCPTT imminent peril group call to a group homed in the IWF and the MCPTT client is not already affiliated to the MCPTT group homed in the IWF; and
- on receipt of a SIP MESSAGE request from an MCPTT server serving an MCPTT user when the MCPTT user initiates an MCPTT emergency alert targeted to an MCPTT group homed in the IWF and the MCPTT client is not already affiliated to the MCPTT group homed in the IWF.

9.2 Procedures

9.2.1 IWF procedures towards the MCPTT system

9.2.1.1 General

The IWF procedures towards the MCPTT system consist of:

- procedures towards the MCPTT system of an IWF serving the user homed in the IWF; and
- procedures of an IWF owning a group that is visible to the MCPTT system.

9.2.1.2 Procedures towards the MCPTT system of an IWF serving the user homed in the IWF

9.2.1.2.1 General

The procedures towards the MCPTT system of an IWF serving the user homed in the IWF consist of:

- 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;
- 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 automatic affiliation to configured groups procedure.

9.2.1.2.2 Stored information

The IWF maintains information equivalent to that defined in TS 24.379 [29] clause 9.2.2.2.2.

NOTE: The virtual data structure referenced in this clause is for information only. Implementors may choose other means to track affiliation status for users homed in the IWF. References to the elements of this virtual data structure are made in other clauses with the understanding that implementors choosing not to use this virtual data structure will take other appropriate actions.

9.2.1.2.3 Procedure for handling affiliation status change of a user homed in the IWF

When the IWF determines that affiliation status should change for a user homed in the IWF, the IWF performing the participating role:

1) shall determine the served MCPTT ID associated with the user homed in the IWF;
2) shall determine the candidate expiration interval for the affiliation according to IETF RFC 3903 [21];
3) shall determine the served MCPTT client ID associated with the user homed in the IWF;
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 clause 9.2.1.2.2; 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) 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 determined by the IWF to be a group to which the user homed in the IWF is to be affiliated:

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 determined by the IWF to be a group to which the user homed in the IWF is not to be affiliated:

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 determined by the IWF to be a group to which the user homed in the IWF is to be affiliated:

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 the 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 be based on service provider policy reduce the candidate MCPTT group IDs to that equal to N2;

NOTE: The service provider policy can determine to remove an MCPTT group ID based on the importance or priority of the MCPTT group or some other policy to determine which groups are preferred.

8) 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;

9) 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;

10) shall perform the procedures specified in clause 9.2.1.2.6 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.

9.2.1.2.4 Receiving subscription to affiliation status procedure

Upon receiving a SIP SUBSCRIBE request such that:

1) the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the IWF performing the terminating participating role serving the user homed in the IWF;

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 associated with a user homed in the IWF performing the terminating participating role;

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

4) the Event header field of the SIP SUBSCRIBE request contains the "presence" event type;

the IWF performing the terminating participating role:

1) if the IWF does not support receiving a SIP SUBSCRIBE request to the affiliation status of a user homed in the IWF, the IWF shall generate and send a SIP 501 (Not Implemented) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [3], IETF RFC 6665 [25], and shall skip the remainder of this procedure;

2) 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;

3) if the Request-URI of the SIP SUBSCRIBE request contains the public service identity identifying the IWF performing the terminating participating role serving the user homed in the IWF, 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 not authorized to subscribe to the affiliation status of the user homed in the IWF, 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 [3], IETF RFC 6665 [25].

For the duration of the subscription, the IWF performing the terminating participating role shall notify the subscriber about changes of the information of the served MCPTT ID, as described in clause 9.2.1.2.5.

9.2.1.2.5 Sending notification of change of affiliation status procedure

In order to notify the subscriber about changes of the served MCPTT ID, the IWF:

NOTE: the served MCPTT ID identifies the user homed in the IWF whose affiliation status has been subscribed.

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 clause 9.2.1.2.2; 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 3GPP TS 24.379 [29], clause 9.3.1 and the served list of the MCPTT client information entries with the following clarifications:

   a) the IWF shall not include information from an MCPTT group information entry with the expiration time already expired;

   b) the IWF shall not include information from an MCPTT group information entry with the affiliation status set to the "deaffiliated" state; and

   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 3GPP TS 24.379 [29], clause 9.3.2, the IWF shall restrict the application/pidf+xml MIME body according to the application/simple-filter+xml MIME body; and

4) send a SIP NOTIFY request according to 3GPP TS 24.229 [3], and IETF RFC 6665 [25] for the subscription created in clause 9.2.1.2.4. In the SIP NOTIFY request, the IWF shall include the generated application/pidf+xml MIME body indicating per-user affiliation information.

9.2.1.2.6 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 users homed in the same IWF and/or to several MCPTT groups owned by the same MCPTT server is not supported in this version of the specification.

In order:

- to send an affiliation request of a user homed in the IWF to a handled MCPTT group ID;

- to send a de-affiliation request of a user homed in the IWF from a handled MCPTT group ID; or
- to send an affiliation request of a user homed in the IWF to a handled MCPTT group ID due to near expiration of the previously published information;

the IWF shall generate a SIP PUBLISH request according to 3GPP TS 24.229 [3], IETF RFC 3903 [21] and IETF RFC 3856 [24]. In the SIP PUBLISH request, the IWF:

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 MCPTT ID associated with the user homed in the IWF;
3) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [3]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];
4) if sending an affiliation request, shall set the Expires header field according to IETF RFC 3903 [21], 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 [14].

5) if sending a de-affiliation request, shall set the Expires header field according to IETF RFC 3903 [21], to zero;
6) shall include a P-Asserted-Identity header field set to the public service identity of the IWF according to 3GPP TS 24.229 [3];
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 clause 9.2.1.2.2; and
   b) the MCPTT ID of the MCPTT user information entry is equal to the MCPTT ID associated with the user homed in the IWF;

   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 for a user homed in the IWF constructed according to 3GPP TS 24.379 [29], clause 9.3.1.2. The IWF shall indicate all MCPTT client IDs associated with the user homed in the IWF, 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 IWF shall set the <p-id> child element of the <presence> root element to the current p-id.

The IWF shall not include the "expires" attribute in the <affiliation> element.

The IWF shall send the SIP PUBLISH request according to 3GPP TS 24.229 [3].

If timer F expires for the SIP PUBLISH request sent for a (de)affiliation request of the user homed in the IWF to the MCPTT group ID or upon receiving a SIP 3xx, 4xx, 5xx or 6xx response to the SIP PUBLISH request, the IWF:

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.

9.2.1.2.7 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 users homed in the same IWF is not supported in this version of the specification.

In order to discover whether a user homed in the IWF was successfully affiliated to a handled MCPTT group in the MCPTT server owning the handled MCPTT group, the IWF shall generate an initial SIP SUBSCRIBE request according to 3GPP TS 24.229 [3], IETF RFC 3856 [24], and IETF RFC 6665 [25].

In the SIP SUBSCRIBE request, the IWF:

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 IWF:

   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 MCPTT ID associated with the user homed in the IWF;

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

4) if the IWF wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [25], 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 [14].

5) if the IWF wants to fetch the current state only, shall set the Expires header field according to IETF RFC 6665 [25], 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 3GPP TS 24.379 [29], clause 9.3.2, indicating the MCPTT ID associated with the user homed in the IWF.

The IWF shall send the SIP SUBSCRIBE request according to 3GPP TS 24.229 [3].

In order to re-subscribe or de-subscribe, the IWF shall generate an in-dialog SIP SUBSCRIBE request according to 3GPP TS 24.229 [3], IETF RFC 3856 [24], and IETF RFC 6665 [25]. In the SIP SUBSCRIBE request, the IWF:

1) if the IWF wants to receive the current status and later notification, shall set the Expires header field according to IETF RFC 6665 [25], 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 [14].

2) if the MCPTT server wants to de-subscribe, shall set the Expires header field according to IETF RFC 6665 [25], 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 [3], IETF RFC 3856 [24], and IETF RFC 6665 [25], if the SIP NOTIFY request contains an application/pidf+xml MIME body indicating per-group affiliation information constructed according to 3GPP TS 24.379 [29], clause 9.3.1, then the IWF:

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 MCPTT ID associated with the user homed in the IWF;

   c) an <affiliation> child element of the <status> element of the <tuple> element;

   d) the "client" attribute of the <affiliation> element indicating the MCPTT client ID associated with the user homed in the IWF; and

   e) 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 MCPTT client ID associated with the user homed in the IWF;

      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 MCPTT ID associated with the user homed in the IWF; and

      iv) the MCPTT user information entry is in the list of MCPTT user information entries described in clause 9.2.1.2.2; and

   b) shall set the affiliation status of the MCPTT group information entry to "affiliated"; and

   c) 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;

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 the MCPTT client ID associated with the user homed in the IWF;

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 the MCPTT ID associated with the user homed in IWF; and

d) the MCPTT user information entry is in the list of MCPTT user information entries described in clause 9.2.1.2.2; 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 MCPTT ID associated with the user homed in the IWF;

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 MCPTT client ID associated with the user homed in the IWF;

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 the MCPTT client ID associated with the user homed in the IWF;

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 the MCPTT ID associated with the user homed in the IWF; and

d) the MCPTT user information entry is in the list of MCPTT user information entries described in clause 9.2.1.2.2; 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 MCPTT ID associated with the user homed in the IWF;

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 MCPTT client ID associated with the user homed in the IWF;

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.

9.2.1.2.8 Affiliation status determination

This clause is referenced from other procedures.

If the IWF performing the participating role needs to determine the affiliation status of a user homed in the IWF to an MCPTT group, the IWF performing the participating role:

1) shall determine the client and MCPTT client ID associated with the user homed in the IWF;

2) shall find the user information entry in the list of MCPTT user information entries described in clause 9.2.1.2.2 such that the MCPTT ID of the MCPTT user information entry is equal to the MCPTT ID associated with the user homed in the IWF;

   a) if the applicable MCPTT group information entry cannot be found, then the IWF performing the participating role shall determine that the user homed in the IWF is not affiliated to the MCPTT group at the determined client and the skip the rest of the steps;

3) 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 determined MCPTT client ID;

   a) if the applicable MCPTT client information entry cannot be found, then the IWF performing the participating role shall determine that the user homed in the IWF is not affiliated to the MCPTT group at the determined client and the skip the rest of the steps;

4) 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 user homed in the IWF at the determined client is 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 user homed in the IWF at the determined client to is not 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 user homed in the IWF at the determined client is not affiliated to the targeted MCPTT group.

9.2.1.2.9 Affiliation status change by implicit affiliation

This clause is referenced from other procedures.

Upon determining that a user homed in the IWF is to be implicitly affiliated to an MCPTT group as per the triggers defined in clause 9.1, the IWF performing the participating role:

1) shall determine the served MCPTT client ID as being the MCPTT ID associated with the user homed in the IWF;

2) shall determine the MCPTT group ID to which the user homed in the IWF is to be implicitly affiliated;

3) shall determine the served MCPTT ID as being the MCPTT ID associated with the user homed in the IWF;

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 clause 9.2.1.2.2; 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 be 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 importance or priority of other MCPTT groups, received SIP requests containing an authorised request for originating a priority call as determined by clause 6.6.2.1.4.2 or other policy to determine which MCPTT groups are preferred.

10) if the determined MCPTT group ID cannot be added to the candidate list of the MCPTT group information entries due to exceeding the N2 limit for the user homed in the IWF, 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.

9.2.1.2.10 Implicit affiliation status change completion

This clause is referenced from other procedures.

If the IWF performing the participating role has received a SIP 2xx response from the controlling MCPTT function to a SIP request that had triggered an affiliation status change by implicit affiliation as per clause 9.2.1.2.9, the IWF performing the participating role:

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 clause 9.2.1.2.9 to "affiliated"; and

2) shall perform the procedures specified in clause 9.2.1.2.5 for the MCPTT ID associated with the user homed in the IWF.

9.2.1.2.11 Implicit affiliation status change cancellation

This clause is referenced from other procedures.

If the IWF performing the participating role for a user homed in the IWF receives a SIP 4xx, 5xx or 6xx response from the controlling MCPTT function to a SIP request that had triggered an affiliation status change by implicit affiliation as per clause 9.2.1.2.9, the IWF performing the participating role:

1) shall remove the MCPTT group ID entry added by the procedures of clause 9.2.1.2.9 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 associated with the user homed in the IWF; 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 associated with the user homed in the IWF.

9.2.1.2.12 Automatic affiliation to configured groups procedure

This clause is referenced from other procedures.

When the IWF determines that automatic affiliation of a user homed in the IWF to configured groups is needed, the IWF shall perform procedures 9.2.1.2.6 and 9.2.1.2.7 for the user homed in the IWF and the targeted groups.

9.2.1.3 Procedures of MCPTT server owning the MCPTT group

9.2.1.3.1 General

The procedures of the IWF 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;
- affiliation status change by implicit affiliation procedure;
- receiving subscription to group dynamic data procedure and;
- sending notification of change of group dynamic data procedure.

9.2.1.3.2 Stored information

The IWF maintains information equivalent to that defined in clause 9.2.1.3.2.

NOTE: The virtual data structure referenced in this clause is for information only. Implementors may choose other means to track affiliation status to groups owned by the IWF. References to the elements of this virtual data structure are made in other clauses with the understanding that implementors choosing not to use this virtual data structure will take other appropriate actions.

9.2.1.3.3 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 IWF owning 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 [3]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

4) the Event header field of the SIP PUBLISH request contains the "presence" event type; and

5) The SIP PUBLISH request contains an application/pidf+xml MIME body indicating per-group affiliation information constructed according to 3GPP TS 24.379 [29], clause 9.3.1.2, with the IWF acting as the controlling MCPTT function;

then the IWF:

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 IWF, shall reject the SIP PUBLISH request with SIP 403 (Forbidden) response to the SIP PUBLISH request according to 3GPP TS 24.229 [3], IETF RFC 3903 [21] and IETF RFC 3856 [24] 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 [3], IETF RFC 3903 [21] and IETF RFC 3856 [24] 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 [3], IETF RFC 3903 [21]. In the SIP 200 (OK) response, the IWF:

   a) shall set the Expires header field according to IETF RFC 3903 [21], 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 clause 9.2.1.3.2; 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 handled 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 clause 9.2.1.3.5 for the served MCPTT group ID.

9.2.1.3.4 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 IWF 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 IWF owning 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 [3]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

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 3GPP TS 24.379 [29], clause 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 IWF:

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 IWF, shall reject the SIP SUBSCRIBE request with SIP 403 (Forbidden) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [3], IETF RFC 3903 [21] and IETF RFC 3856 [24] 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 [3], IETF RFC 3903 [21] and IETF RFC 3856 [24] and skip the rest of the steps; and

6) shall generate and send a SIP 200 (OK) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [3], IETF RFC 6665 [25].

For the duration of the subscription, the IWF shall notify subscriber about changes of the information of the served MCPTT ID, as described in clause 9.2.1.3.5.

9.2.1.3.5 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 IWF:

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 clause 9.2.1.3.2; 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 3GPP TS 24.379 [29], clause 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 procedure is invoked by procedure in clause 9.2.1.3.3 where the handled p-id was identified, the IWF shall set the <p-id> child element of the <presence> 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 [3], and IETF RFC 6665 [25] for the subscription created in clause 9.2.1.3.4. In the SIP NOTIFY request, the IWF shall include the generated application/pidf+xml MIME body indicating per-group affiliation information.

9.2.1.3.6 Implicit affiliation eligibility check procedure

This clause 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 IWF performing the controlling role to check on the eligibility of the MCPTT user to be implicitly affiliated to the MCPTT group, the IWF performing the controlling role:

1) shall perform the procedures of clause 9.2.1.3.8 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 clause 9.2.1.3.8, shall consider the MCPTT user to be eligible for implicit affiliation to the MCPTT group.

9.2.1.3.7 Affiliation status change by implicit affiliation procedure

This clause 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 IWF performing the controlling role to perform an implicit affiliation to, the IWF performing the controlling role:

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 clause 9.2.1.3.2 with the IWF acting as the controlling MCPTT function; 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 clause 9.2.1.3.5 for the served MCPTT group ID.

9.2.1.3.8 Affiliation eligibility check procedure

This clause 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 IWF performing the controlling role to check on the eligibility of the MCPTT user to be affiliated to the MCPTT group, the IWF performing the controlling role:

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 IWF, 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 clause 9.2.1.3.2, with the IWF acting as the controlling MCPTT function, 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.

9.2.1.3.9 Receiving subscription to group dynamic data procedure

Upon receiving a SIP SUBSCRIBE request such that:

1) Request-URI of the SIP SUBSCRIBE request contains the public service identity of the IWF owning 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 [3]), in a P-Asserted-Service header field according to IETF RFC 6050 [7];

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-group dynamic data of presence event package notification information according to 3GPP TS 24.379 [29] clause 9.3.2 indicating the same MCPTT group 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 IWF:

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 IWF, shall reject the SIP SUBSCRIBE request with SIP 403 (Forbidden) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [3], IETF RFC 3903 [21] and IETF RFC 3856 [24] and skip the rest of the steps;

5) if the IWF does not support receiving a SIP SUBSCRIBE request to the group dynamic data of a group owned by the IWF, the IWF shall generate and send a SIP 501 (Not Implemented) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [3], IETF RFC 6665 [25], and skip the rest of the steps;

6) if the handled MCPTT ID is not authorized to subscribe to group dynamic data 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 [3], IETF RFC 3903 [21] and IETF RFC 3856 [24] and skip the rest of the steps; and

7) shall generate a SIP 200 (OK) response to the SIP SUBSCRIBE request according to 3GPP TS 24.229 [3], IETF RFC 6665 [25].

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 clause 9.2.1.3.10.

9.2.1.3.10 Sending notification of change of group dynamic data procedure

In order to notify the subscriber identified by the handled MCPTT ID about changes of the per-group dynamic data of the served MCPTT group ID, the IWF:

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 clause 9.2.1.3.2; and

b) the MCPTT group ID of the MCPTT group information entry is equal to the served MCPTT group ID;

2) shall generate an application/pidf+xml MIME body indicating per-group dynamic data according to 3GPP TS 24.379 [29], clause 9.3.1 with the following clarifications:

a) the IWF shall include the "expires" attribute in the <affiliation> element; and

3) shall send a SIP NOTIFY request according to 3GPP TS 24.229 [3], and IETF RFC 6665 [25] for the subscription created in clause 9.2.1.3.8. In the SIP NOTIFY request, the IWF shall include the generated application/pidf+xml MIME body indicating per-group dynamic data.

10 Call signalling - group call

10.1 Prearranged group call

10.1.2 Client derived procedures

10.1.2.1 IWF originating procedures

This clause is referred to by other clauses.

To establish an MCPTT prearranged group session, the IWF performing the participating role shall generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [3], with the clarifications given below.

The IWF performing the participating role:

1) if originating an MCPTT emergency group call or originating an MCPTT prearranged group call and the MCPTT emergency state is already set, the IWF performing the participating role shall comply with the procedures in clause 6.4.1.1;

2) if originating an MCPTT imminent peril group call, the IWF performing the participating role shall comply with the procedures in clause 6.4.1.6;

3) if originating a broadcast group call, the IWF performing the participating role shall include in the application/vnd.3gpp.mcptt-info+xml MIME body the <broadcast-ind> element set to "true" as defined in 3GPP TS 24.379 [29], clause F.1;

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 [9];

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 [5];

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 [5];

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 [6]. It is recommended that the "refresher" header field parameter is omitted. If included, the "refresher" header field parameter shall be set to "uac";

9) if the emergency group state for this group is set to "MEG 2: in-progress" or "MEG 4: confirm-pending", the IWF performing the participating role shall include the Resource-Priority header field and comply with the procedures in clause 6.4.1.2;

10) if the 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 clause 6.4.1.8;

11) 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 "prearranged";

   b) the <mcptt-request-uri> element set to the group identity;

   c) the <mcptt-client-id> element set to a value determined by the IWF; and

NOTE 1: How the IWF determines the value of the <mcptt-client-id> element is out of scope of the present document.

   d) if the group identity can be determined to be a TGI and if the IWF performing the participating role can associate the TGI with a MCPTT group ID, the <associated-group-id> element set to the MCPTT group ID;

NOTE 2: The MCPTT ID will be inserted into the body of the SIP INVITE request by the referring clause.

NOTE 3: The text "can associate the TGI with a MCPTT group ID" means that the IWF performing the participating role is able to determine that there is a constituent group of the temporary group that it is a member of.

NOTE 4: The IWF performing the participating role is informed about temporary groups and regouping of MCPTT groups that the users homed in the IWF are members of as specified in 3GPP TS 24.481 [16].

NOTE 5: If the TGI has several MCPTT groups as constituent groups, where the user homed in the IWF is a member, the IWF performing the participating role selects one of those MCPTT groups.

12) shall include an SDP offer according to 3GPP TS 24.229 [3] with the clarifications given in clause 6.1.1; and

13) if an implicit floor request is required, shall indicate this as specified in clause 6.7; and shall skip the rest of the steps.

On receiving a SIP 2xx response to the SIP INVITE request, the IWF performing the participating role:

1) shall interact with the user plane as specified in 3GPP TS 29.380 [31];

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 IWF performing the participating role shall perform the actions specified in clause 6.4.1.4; and

3) may subscribe to the conference event package as specified in clause 10.3.

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 IWF performing the participating role shall perform the actions specified in clause 6.4.1.5.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the IWF performing the participating role shall follow the actions specified in clause 6.4.1.9.

10.1.2.2 IWF performing the participating role terminating procedures

This clause is referenced from other procedures.

In the procedures in this clause:

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.

The IWF performing the participating role:

1) may reject the SIP INVITE request,

NOTE: The conditions under which the IWF rejects the request are out of scope of the present document.

2) if the SIP INVITE request is rejected in step 1), shall respond towards the controlling MCPTT function either with an appropriate reject code as specified in 3GPP TS 24.229 [3] and warning texts as specified in clause 4.2.2 or with a SIP 480 (Temporarily unavailable) response and skip the rest of the steps of this clause;

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) shall set the MCPTT emergency group state to "MEG 2: in-progress";

   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"; 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", shall set the MCPTT imminent peril group state to "MIG 2: in-progress";

5) shall perform the automatic commencement procedures specified in clause 6.2.1 if one of the following conditions are met:

   a) if the SIP INVITE request contains an Answer-Mode header field with the value "Auto" and IWF is configured for automatic commencement mode for receiving the call;

   b) if the SIP INVITE request contains an Answer-Mode header field with the value "Auto" and IWF is configured to allow automatic commencement mode for receiving the call; or

   c) SIP INVITE request contains an Answer-Mode header field with the value "Manual" and IWF is not configured to allow manual commencement mode for receiving the call;

6) shall perform the manual commencement procedures specified in clause 6.2.2 if one of the following conditions are met:

   a) if the SIP INVITE request contains an Answer-Mode header field with the value "Manual" and IWF is configured for manual commencement mode for receiving the call;

   b) if the SIP INVITE request contains an Answer-Mode header field with the value "Manual" and IWF is configured to allow manual commencement mode for receiving the call; or

   c) SIP INVITE request contains an Answer-Mode header field with the value "Automatic" and IWF is not configured to allow automatic commencement mode for receiving the call; and

7) when the SIP 200 (OK) response to the SIP INVITE request is sent, may subscribe to the conference event package as specified in clause 10.3.

10.1.2.3 MCPTT upgrade to in-progress emergency or imminent peril

This clause is referenced from other procedures.

To upgrade the MCPTT group session to an emergency condition or an imminent peril condition on an MCPTT prearranged group, the IWF performing the participating role shall perform the steps below.

1) if the request is to upgrade the MCPTT group session to an MCPTT emergency call, the IWF performing the participating role:

   a) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.1.1; and

   b) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.1.2.

2) if the MCPTT user has requested to upgrade the MCPTT group session to an MCPTT imminent peril call, the IWF performing the participating role:

   a) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.1.6; and

   b) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.1.8;

3) 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 [3] with the clarifications specified in clause 6.1.1;

NOTE: The SIP re-INVITE request can be sent within an on-demand session.

4) if an implicit floor request is required, shall indicate this as specified in clause 6.7; and

5) shall exit the procedure in the present clause.

On receiving a SIP 2xx response to the SIP re-INVITE request the IWF performing the participating role:

1) shall perform the actions specified in clause 6.4.1.4.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the IWF performing the participating role shall follow the actions specified in clause 6.4.1.9.

On receiving a SIP 4xx response, SIP 5xx response or a SIP 6xx response to the SIP re-INVITE request the IWF performing the participating role shall perform the actions specified in clause 6.4.1.5.

10.1.2.4 MCPTT in-progress emergency cancel

This clause is referenced from other procedures.

To cancel the in-progress emergency condition on a prearranged MCPTT group, the IWF performing the participating role shall generate a SIP re-INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [3], with the clarifications given below.

The IWF performing the participating role:

1) shall, if cancelling an in-progress emergency condition and optionally an MCPTT emergency alert originated by the user homed in the IWF, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.1.3;

2) 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;

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

4) 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 [9];

5) shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [3] with the clarifications specified in clause 6.1.1;

6) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.1.2; and

7) shall exit the procedure in the present clause.

On receiving a SIP 2xx response to the SIP re-INVITE request, the IWF performing the participating role:

1) shall interact with the user plane as specified in 3GPP TS 29.380 [31];

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 clause 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 IWF performing the participating role shall follow the actions specified in clause 6.4.1.9 with the IWF acting as the MCPTT client.

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 IWF performing the participating role 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: 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.

10.1.2.5 MCPTT in-progress imminent peril cancel

This clause is referenced from other procedures.

To cancel the in-progress imminent peril condition on a prearranged MCPTT group, the IWF performing the participating role shall generate a SIP re-INVITE request by following the procedures specified in 3GPP TS 24.229 [3], with the clarifications given below.

The IWF performing the participating role:

1) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.1.7;

2) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.1.8;

3) 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;

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

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 [9];

6) shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [3] with the clarifications specified in clause 6.1.1; and

7) shall exit the procedure in the present clause.

On receiving a SIP 2xx response to the SIP re-INVITE request, the IWF performing the participating role:

1) shall interact with the user plane as specified in 3GPP TS 29.380 [31];

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 IWF performing the participating role shall set the MCPTT imminent peril group state as "MIG 2: in-progress".

NOTE: This is the case where the IWF performing the participating role requested the cancellation of the MCPTT imminent peril in-progress state and was rejected.

10.1.2.6 Reception of SIP re-INVITE request

This clause is referred to by other clauses.

The IWF:

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) shall set the MCPTT emergency group state to "MEG 2: in-progress";

   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";

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) 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) if the <mcpttinfo> element containing the <mcptt-Params> element contains an <alert-ind> element set to "false":

      i) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body including an <originated-by> element:

         A) if the MCPTT ID contained in the <originated-by> element is the MCPTT ID of the receiving user homed in the IWF, shall set the MCPTT emergency alert state to "MEA 1: no-alert";

   b) shall set the MCPTT emergency group state to "MEG 1: no-emergency"; and

   c) 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) 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";

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 [3];

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

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 SIP 200 (OK) response; and

8) 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 [3] with the clarifications given in clause 6.1.2.

10.1.3 IWF participating role procedures

10.1.3.1 Originating procedures

10.1.3.1.1 On demand prearranged group call

Editor's Note: Behaviour for cases where the IWF affiliates on behalf of its LMR users is FFS.

In this clause, the IWF originates a prearranged group session on behalf of an LMR user.

NOTE 1: How the IWF determines the MCPTT ID of the calling user is out of scope of the present document.

The IWF, performing the originating participating function:

1) if the user identified by the MCPTT ID is not affiliated to the group as determined by clause 9.2.1.2.8 and this is an authorised request for originating a priority call as determined by clause 6.6.2.1.4.2, shall perform the actions specified in clause 9.2.1.2.9 for implicit affiliation;

2) shall determine the public service identity of the controlling MCPTT function associated with the group identity of the group on which the call is to be originated;

NOTE 2: How the IWF discovers the public service identity of the controlling MCPTT function associated with the group identity is out of scope of the present document.

3) shall generate a SIP INVITE request as specified in clause 10.1.2.1;

4) shall modify the SIP INVITE request as specified in clause 6.6.2.1.2;

5) may insert the calling user's location information into an application/vnd.3gpp.mcptt-location-info+xml MIME body to be included in the outgoing SIP request;

6) shall set the Request-URI to the public service identity of the controlling MCPTT function associated with the group identity;

7) 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;

8) shall update the SDP as specified in clause 6.6.2.1.1.1; and

9) shall send the SIP INVITE request to the controlling MCPTT function as specified in 3GPP TS 24.229 [3].

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

1) shall generate a SIP INVITE request as specified in clause 6.6.2.1.5;

2) shall include an SDP offer based upon the SDP offer in the SIP INVITE request generated by the IWF in the step above; and

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

Upon receipt of a SIP 2xx response in response to the above SIP INVITE request, the IWF performing the participating role:

NOTE 3: If an <MKFC-GKTPs> element is received, the IWF ignores that element.

1) if the procedures of clause 9.2.1.2.9 for implicit affiliation were performed in the present clause, shall complete the implicit affiliation by performing the procedures of clause 9.2.1.2.10;

2) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [6].

3) shall perform the steps for SIP 2xx as specified in clause 10.1.2.1.

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

1) if the implicit affiliation procedures of clause 9.2.1.2.9 were invoked in this procedure, shall perform the procedures of clause 9.2.1.2.11; and

2) shall perform the steps for the received SIP 4xx, 5xx or 6xx as specified in clause 10.1.2.1.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the IWF shall perform the steps for the received SIP INFO in clause 10.1.2.1.

10.1.3.1.2 Sending of a SIP re-INVITE request towards MCPTT controlling function

Upon a need to send a SIP re-INVITE request for an MCPTT session identifying an on-demand prearranged MCPTT group session, the IWF performing the participating role:

1) if the request is for an upgrade to an in-progress emergency or an imminent peril, shall perform the steps in clause 10.1.2.3;

2) if the request is for a cancellation of an in-progress emergency, shall perform the steps in clause 10.1.2.4;

3) if the request is for a cancellation of an in-progress imminent peril, shall perform the steps in clause 10.1.2.5;

4) shall include the MCPTT ID of the originating user in <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP re-INVITE request;

NOTE 1: How the IWF determines the MCPTT ID of a user homed in the IWF is out of scope of the present document.

5) shall include in the SIP re-INVITE request an SDP offer as specified in clause 6.6.2.1.1;

6) if the SIP re-INVITE requires a Resource-Priority header field, shall include a Resource-Priority header field according to 6.4.1.11; and

7) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [3].

Upon receipt of a SIP 2xx response to the above SIP re-INVITE request, the IWF performing the participating role:

1) shall interact with the media plane as specified in 3GPP TS 29.380 [31];

2) if the request in the present clause above is for an upgrade for emergency or imminent peril, shall follow the procedures for SIP 200 (OK) response as specified in clause 10.1.2.3;

3) if the request in the present clause above is for an in-progress emergency cancel, shall follow the procedures for SIP 200 (OK) response as specified in clause 10.1.2.4; and

4) if the request in the present clause above is for an in-progress imminent peril cancel, shall follow the procedures for SIP 200 (OK) response as specified in clause 10.1.2.5.

Upon receipt of a SIP 403 (Forbidden) response to the above SIP re-INVITE request, the IWF performing the participating role shall interact with the media plane as specified in 3GPP TS 29.380 [31].

On receiving a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP re-INVITE request, the IWF performing the participating role:

1) if the request in the present clause above is for an upgrade for emergency or imminent peril, shall follow the procedures for SIP 4xx, SIP 5xx and SIP 6xx responses as specified in clause 10.1.2.3;

2) if the request in the present clause above is for an in-progress emergency cancel, shall follow the procedures for SIP 4xx, SIP 5xx and SIP 6xx responses as specified in clause 10.1.2.4; or

3) if the request in the present clause above is for an in-progress imminent peril cancel, shall follow the procedures for SIP 4xx, SIP 5xx and SIP 6xx responses as specified in clause 10.1.2.5.

Upon receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing session, the IWF performing the participating role:

1) if the SIP re-INVITE request in the present clause above is for an upgrade for emergency or imminent peril, shall follow the procedures for SIP INFO as specified in clause 10.1.2.3;

2) if the SIP re-INVITE request in the present clause above is for an in-progress emergency cancel, shall follow the procedures for SIP INFO as specified in clause 10.1.2.4; or

3) if the SIP re-INVITE request in the present clause above is for an in-progress imminent peril cancel, shall follow the procedures for SIP INFO as specified in clause 10.1.2.5.

10.1.3.2 Terminating Procedures

In the procedures in this clause:

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 INVITE request for terminating participating MCPTT function", the IWF performing the participating role:

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 IWF performing the participating role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14], 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 IWF performing the participating role 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 clause 4.4, and shall not continue with the rest of the steps;

3) may 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the MCPTT server and shall not continue with the rest of the steps; and

NOTE: If an <MKFC-GKTPs> element is received, the IWF ignores it.

4) shall perform the steps in 3GPP TS 24.379 [29], clause 10.1.2.1.2.

10.1.3.3 IWF participating role ending group call

10.1.3.3.1 IWF ending group call on-demand

When the IWF performing the participating role determines it has to send a SIP BYE request, the IWF shall follow the procedures as specified in clause 6.6.2.1.3.

10.1.3.4 End group call at the IWF performing the participating role

10.1.3.4.1 Receipt of SIP BYE request for private call on-demand

Upon receiving a SIP BYE request from the controlling MCPTT function, the IWF performing the participating role shall follow the procedures as specified in clause 6.6.2.2.2.1.

10.1.3.5 Re-join procedures

10.1.3.5.1 Originating procedures - on demand prearranged group call

To rejoin an on demand prearranged group call, the IWF performing the participating role shall follow the procedures specified in clause 10.1.3.1.1 with the clarification that the Request-URI of the SIP INVITE request shall contain a URI of the MCPTT session identity to re-join.

10.1.3.6 Reception of a SIP re-INVITE request for terminating a priority call

In the procedures in this clause:

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 group containing an emergency indication or imminent peril indication, the IWF performing the participating role:

1) shall perform the steps in clause 10.1.2.6;

2) shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

3) shall send the SIP 200 (OK) response according to 3GPP TS 24.229 [3].

10.1.4 IWF Controlling role procedures

10.1.4.1 Originating Procedures

10.1.4.1.1 INVITE targeted to an MCPTT client

This clause describes the procedures for inviting an MCPTT user to an MCPTT session. The procedure is initiated by the IWF performing the controlling role as the result of a request from the LMR system or an action in clause 10.1.4.2 or as the result of receiving a SIP 403 (Forbidden) response as described in this clause.

The IWF performing the controlling role:

1) shall generate a SIP INVITE request as specified in clause 6.6.3.1.1;

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 IWF performing the controlling role 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 IWF performing the controlling role;

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 clause 6.6.3.1.1 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 TS 24.379 [29], clause 6.3.3.1.1, with the IWF acting as the controlling MCPTT function;

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

a) shall include a Resource-Priority header field populated with the values for an MCPTT emergency group call as specified in clause 6.6.3.1.12.

b) if the IWF needs to set the group state to emergency:

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 IWF needs to set an emergency alert and the MCPTT group is authorised for the initiation of MCPTT emergency alerts as determined by the procedures of clause 6.6.3.1.8.1, 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 clause 6.6.3.1.7. 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 IWF performing the controlling role:

a) shall include a Resource-Priority header field populated with the values for an MCPTT imminent peril group call as specified in clause 6.6.3.1.12; 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"; and

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

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 IWF performing the controlling role:

1) shall send a SIP PRACK request towards the MCPTT client according to 3GPP TS 24.229 [3].

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the IWF performing the controlling role:

1) shall interact with the media plane as specified in 3GPP TS 29.380 [31] clause 6.3;

2) shall send a SIP NOTIFY request to all MCPTT participants with a subscription to the conference event package as specified in clause 10.3; and

3) shall increment the local counter of the number of SIP 200 (OK) responses received from invited members, by 1.

10.1.4.1.2 INVITE targeted to the non-controlling MCPTT function of an MCPTT group

The IWF performing the controlling role:

1) shall generate a SIP INVITE request as specified in clause 6.6.3.1.1;

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 IWF performing the controlling role;

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 IWF performing the controlling role;

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; and

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

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 [20];

NOTE 1: The application/resource-lists+xml MIME body contains MCPTT IDs identifying MCPTT users in a partner MCPTT system that need to be invited to the prearranged group call in case of group regrouping using interrogating method as specified in 3GPP TS 23.379 [2] clause 10.6.2.4.2.

then the IWF performing the controlling role:

1) shall check if the number of members of the MCPTT group exceeds the maximum participants allowed by the IWF performing the controlling role. If exceeded, the IWF performing the controlling role shall invite only enough members from the application/resource-lists+xml MIME body to reach the maximum allowed by the IWF performing the controlling role; and

NOTE 2: The IWF determines 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 clause using the list of MCPTT IDs in URI-List.

Upon receiving a SIP 200 (OK) response for the SIP INVITE request the IWF performing the controlling role:

1) shall interact with the media plane as specified in 3GPP TS 29.380 [31] clause 6.3;

NOTE 3: The procedures executed by the IWF performing the controlling role prior to sending a response to the inviting MCPTT client are specified in clause 10.1.4.2.

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 clause 10.3; 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 IWF performing the controlling role:

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 [3]; and

2) shall interact with the media plane as specified in 3GPP TS 29.380 [31] clause 6.3.

10.1.4.2 Terminating Procedures

In this clause, the IWF is performing the controlling role and is terminating a call from an MCPTT participating function or an MCPTT non-controlling function destined for the IWF. For cases where both the call origination and termination are MCPTT functions, the IWF shall follow 3GPP TS 24.379 [29], clause 10.1.1.4.2, with the IWF acting as the controlling MCPTT function.

In the procedures in this clause:

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) 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;

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) 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 IWF performing the controlling role:

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 IWF performing the controlling role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14] 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 clause 6.6.3.1.8.2, or for originating an MCPTT imminent peril group call as determined by clause 6.6.3.1.8.5, the IWF performing the non-controlling role can, according to local policy, choose to accept the request.

2) shall determine if the media parameters are acceptable 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 3GPP TS 24.379 [29], clause 6.3.3.1.17 with the IWF acting as the controlling MCPTT function;

5) shall retrieve the necessary group document(s) and carry out initial processing as specified in 3GPP TS 24.379 [29], clause 6.3.5.2 with the IWF acting as the controlling MCPTT function;

6) if the result of the initial processing in 3GPP TS 24.379 [29], clause 6.3.5.2 was:

   a) that authorization of the MCPTT ID at a non-controlling MCPTT function of an MCPTT group is required, perform the actions in clause 6.6.3.1.8.7 and do not continue with the rest of the steps in this clause; 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 clause;

7) shall perform the actions as described in 3GPP TS 24.379 [29], clause 6.3.3.2.2 with the IWF acting as the controlling MCPTT function;

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 clause 6.6.3.1.8.2:

   a) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response as specified in clause 6.6.3.1.9; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [3] 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 clause 6.6.3.1.8.5, 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 3GPP TS 24.379 [29], 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 [3] and skip the rest of the steps;

12) void

13) if the received SIP INVITE request contains an application/vnd.3gpp.mcptt-location-info+xml MIME body with a <Report> element included in the <location-info> root element, the IWF performing the controlling role can remember the location information contained in the <location-info> root element;

14) 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 3GPP TS 24.379 [29], clause 6.3.6, with the IWF acting as the controlling MCPTT function;

      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 clause 6.6.3.1.8.2 or MCPTT imminent peril group call as determined by steps clause 6.6.3.1.8.5 and is determined to not be eligible for implicit affiliation as specified in clause 9.2.1.3.6;

      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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server, 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, 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server and skip the rest of the steps below;

NOTE 2: How the IWF determines whether the MCPTT user is authorized to initiate a prearranged group is out of scope of the present document.

   c) if the received SIP INVITE request contains an authorised request for an MCPTT emergency group call as determined by clause 6.6.3.1.8.2 or MCPTT imminent peril group call as determined by clause 6.6.3.1.8.5 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 clause 9.2.1.3.7;

d) void

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 clause 6.6.3.5;

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 in the IWF:

A) invite each member of the IWF homed group to the group session; and

B) interact with the media plane as specified in 3GPP TS 29.380 [31] clause 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 clause 10.1.4.1.2;

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 clause 6.6.5.3;

ii) if necessary, shall start timer TNG1 (acknowledged call setup timer) according to the conditions stated in clause 6.6.3.3;

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 clause 6.6.3.1.8.1, 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 clause 6.6.3.1.10;

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:

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 clause 10.1.4.1.1; and

vi) shall interact with the media plane as specified in 3GPP TS 29.380 [31] clause 6.3; and

15) 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 3GPP TS 24.379 [29] clause 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 clause 6.6.3.1.8.2 or MCPTT imminent peril group call as determined clause 6.6.3.1.8.5 and is determined to not be eligible for implicit affiliation as specified in clause 9.2.1.3.6;

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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server, 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 clause 6.6.5.2, 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the MCPTT server and skip the rest of the steps below;

c) void

d) if the maximum number of participants allowed by the IWF performing the controlling role 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 clause 10.1.4.4.3, 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's priority and the participant type of the user as well as other information about the user. 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the MCPTT server 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 clause 6.6.3.1.8.2 or MCPTT imminent peril group call as determined by clause 6.6.3.1.8.5 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 clause 9.2.1.3.7;

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 clause 6.6.3.1.8.1, 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 clause 6.6.3.1.10; 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 clause 6.6.3.1.3;

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 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, 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 [3]; and

v) upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31];

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 3GPP TS 24.379 [29], clause 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 29.380 [31]; 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 3GPP TS 24.379 [29] clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, 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 [3];

h) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.379 [29], clause 6.3.3.2.3.2;

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 3GPP TS 24.379 [29] clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

j) shall include in the SIP 200 (OK) response with the warning text set to "123 MCPTT session already exists" as specified in 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

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 29.380 [31] clause 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 [3];

o) shall generate a notification to the MCPTT clients, which have subscribed to the conference event package that the inviting MCPTT User has joined in the MCPTT group session, as specified in clause 6.6.3.4;

NOTE 6: As a group document can potentially have a large content, the IWF performing the controlling role can notify using content-indirection as defined in IETF RFC 4483 [17].

p) shall send a SIP NOTIFY request to each MCPTT client according to 3GPP TS 24.229 [3];

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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server with the warning text containing the mcptt-warn-code set to "149", shall follow the procedures in clause 6.6.3.1.11; and

r) shall not continue with the rest of the clause.

Upon receiving a SIP 183 (Session Progress) response to the SIP INVITE request specified in clause 10.1.4.1 containing a P-Answer-State header field with the value "Unconfirmed" as specified in IETF RFC 4964 [19], 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 3GPP TS 24.379 [29] clause 6.3.3.2.3.2, with the IWF acting as the controlling MCPTT function;

2) shall include the warning text set to "122 too many participants" as specified in 3GPP TS 24.379 [29] clause 4.4 with the IWF acting as the MCPTT server, in the SIP 200 (OK) response, if the prearranged MCPTT group has more than the maximum number of members as allowed by the IWF;

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 3GPP TS 24.379 [29] clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

7) shall interact with the media plane as specified in 3GPP TS 29.380 [31] clause 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 [3];

9) shall generate a notification to the MCPTT clients, which have subscribed to the conference event package that the inviting MCPTT User has joined in the MCPTT group session, as specified in clause 6.6.3.4; 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 [17].

10) shall send a SIP NOTIFY request to each MCPTT client according to 3GPP TS 24.229 [3].

Upon receiving a SIP 183 (Session Progress) response for a SIP INVITE request as specified in clause 10.1.4.1.2 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 clause 10.1.4.1.1, then the IWF performing the controlling role shall wait until the SIP 200 (OK) response has been received to the SIP INVITE request specified in clause 10.1.4.1.2 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 clause 10.1.4.1 that was sent to an affiliated and required group member; 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 required group members; and

3) there is no outstanding SIP 200 (OK) response to a SIP INVITE request sent in clause 10.1.4.1.2 where the SIP 183 (Session Progress) response contained an indication of required group members;

the IWF performing the controlling role:

1) shall stop timer TNG1 (acknowledged call setup timer) as described in clause 6.6.3.3;

2) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the 3GPP TS 24.379 [29] clause 6.3.3.2.3.2, with the IWF acting as the controlling MCPTT function, before continuing with the rest of the steps;

3) shall include the warning text set to "122 too many participants" as specified in 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server in the SIP 200 (OK) response, if all members were not invited because the prearranged MCPTT group has been exceeded the maximum number of members as allowed by the IWF;

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 3GPP TS 24.379 [29] clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

5) shall interact with the media plane as specified in 3GPP TS 29.380 [31] clause 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 [3];

7) shall generate a notification to the MCPTT clients, which have subscribed to the conference event package that the inviting MCPTT user has joined in the MCPTT group session, as specified in clause 6.6.3.4; and

NOTE 10: As a group document can potentially have a large content, the IWF performing the controlling role can notify using content-indirection as defined in IETF RFC 4483 [17].

8) shall send the SIP NOTIFY request to the MCPTT clients according to 3GPP TS 24.229 [3].

Upon:

1) receiving a SIP 200 (OK) response for a SIP INVITE request as specified in clause 10.1.4.1;

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 minimum number of participants that the IWF requires to start a call;

4) the IWF performing the controlling role supports media buffering; and

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

the IWF performing the controlling role according to local policy:

1) shall generate SIP 200 (OK) response to the SIP INVITE request as specified in the 3GPP TS 24.379 [29] clause 6.3.3.2.2, with the IWF acting as the controlling MCPTT function;

2) shall include the warning text set to "122 too many participants" as specified in 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server in the SIP 200 (OK) response, if all members were not invited because the prearranged MCPTT group has exceeded the number of members as allowed by the IWF performing the controlling role;

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 3GPP TS 24.379 [29] clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server;

6) shall interact with the media plane as specified in 3GPP TS 29.380 [31] clause 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 [3];

8) shall generate a notification to the MCPTT clients, which have subscribed to the conference event package that the inviting MCPTT user has joined in the MCPTT group session, as specified in clause 6.6.3.4; and

NOTE 12: As a group document can potentially have a large content, the IWF performing the controlling role can notify using content-indirection as defined in IETF RFC 4483 [17].

9) shall send the SIP NOTIFY request to the MCPTT clients according to 3GPP TS 24.229 [3].

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 required group members, the IWF performing the controlling role shall follow the procedures specified in clause 6.6.3.3.

If timer TNG1 (acknowledged call setup timer) is running and a final SIP 4xx, 5xx or 6xx response is received from an affiliated and required group member, the IWF performing the controlling role shall follow the relevant procedures specified in clause 6.6.3.3.

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 minimum number of group members required by the IWF to start a call; and

3) a final SIP 4xx, 5xx or 6xx response is received from an invited MCPTT client;

then the IWF performing the controlling role 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 [3], 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 clause 6.6.3.1.2, 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 IWF performing the controlling role may invite an additional member of the prearranged MCPTT group as specified in clause 10.1.4.1 that has not already been invited, if the prearranged MCPTT group has less than the maximum number of members as allowed by the IWF, 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 clause 10.1.4.1.2 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 IWF performing the controlling role 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 3GPP TS 24.379 [29] clause 4.4, with the IWF acting as the MCPTT server, the controlling MCPTT function shall follow the procedures in clause 6.6.3.1.11.

10.1.4.3 End group call at the IWF performing the terminating controlling role

Upon receiving a SIP BYE request the IWF performing the controlling role shall follow the procedures as specified in clause 6.6.3.2.1.

10.1.4.4 End group call initiated by the IWF performing the controlling role

10.1.4.4.1 General

This clause describes the procedures of each functional entity for ending the group call initiated by the IWF performing the controlling role.

10.1.4.4.2 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 clause 6.6.7.1, the IWF performing the controlling role, shall follow the procedures in clause 6.6.3.1.2.

10.1.4.4.3 SIP BYE request towards 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 IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.2.

After successful removing the MCPTT client from the MCPTT session, the IWF performing the controlling role may generate a notification to the MCPTT clients, which have subscribed to the conference event package that an MCPTT user has been removed from the MCPTT session, as specified in clause 6.6.3.4 and send the SIP NOTIFY request to the MCPTT client according to 3GPP TS 24.229 [3].

10.1.4.5 Re-join procedures

10.1.4.5.1 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 IWF performing the controlling role:

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 IWF performing the controlling role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14]. 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 clause 6.6.3.1.8.2, or for originating an MCPTT imminent peril group call as determined by clause 6.6.3.1.8.5, with the IWF performing the controlling role 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 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 IWF performing the controlling role and if not, reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps 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 clause 6.6.5.2, 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function. 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 3GPP TS 24.379 [29], clause 6.3.3.2.2, with the IWF acting as the controlling MCPTT function;

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 clause 6.5.3.5, 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 clause 4.4;

Editor's Note: Clause 6.5.3.5 does not exist in the present document, the correct reference is FFS.

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 [3];

10) if <on-network-max-participant-count> as specified in 3GPP TS 24.481 [16] 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 clause 10.1.4.4.3, 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 [16]. 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 3GPP TS 24.379 [29], clause 4.4 with the IWF acting as the controlling MCPTT function. Otherwise, continue with the rest of the steps;

11) shall generate a SIP 200 (OK) response as specified in 3GPP TS 24.379 [29], clause 6.3.3.2.3.2, with the IWF acting as the controlling MCPTT function;

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 3GPP TS 24.379 [29], clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

13) shall interact with media plane as specified in 3GPP TS 29.380 [31] clause 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 [3];

15) shall generate a notification to the MCPTT clients, which have subscribed to the conference event package that the inviting MCPTT User has joined in the MCPTT group session, as specified in clause 6.6.3.4; and

NOTE 4: As a group document can potentially have a large content, the IWF performing the controlling role can notify using content-indirection as defined in IETF RFC 4483 [17].

16) shall send a SIP NOTIFY request to each MCPTT client according to 3GPP TS 24.229 [3].

10.1.4.6 Late call entry initiated by IWF performing the controlling role

When the IWF performing the controlling role is notified that an MCPTT client is newly affiliated or comes back from out of coverage, the IWF performing the controlling role shall invite the MCPTT client to join an ongoing MCPTT group call by following the procedures specified in clause 10.1.4.1.

NOTE: How the IWF is informed when an MCPTT client is coming back from out of coverage is out of scope of present document.

10.1.4.7 Receipt of a SIP re-INVITE request

In the procedures in this clause:

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 IWF performing the controlling role:

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 IWF performing the controlling role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14] 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 IWF performing the controlling role 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 3GPP TS 24.379 [29], clause 6.3.3.1.17, with the IWF acting as the controlling MCPTT function;

3) if the received SIP re-INVITE request contains an unauthorised request for an MCPTT emergency call as determined by clause 6.6.3.1.8.2:

   a) shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response as specified in clause 6.6.3.1.9; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [3] 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 clause 6.6.3.1.8.6, 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 3GPP TS 24.379 [29], 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 [3] 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 clause 6.6.3.1.8.2, the IWF performing the controlling role:

      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 clause 6.6.3.1.8.1, 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 MCPTT members of the group generate a SIP MESSAGE request notification of the MCPTT user's emergency indication as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, 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 [3]; 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 clause 6.6.3.1.10;

NOTE 2: The interactions of TNG2 with the TNG3 (group call timer) are explained in clause 6.6.3.5.2.

C) shall generate SIP re-INVITE requests for the MCPTT emergency group call to the other MCPTT participants of the MCPTT group call as specified in clause 6.6.3.1.3;

D) shall send the SIP re-INVITEs towards the other MCPTT participants of the MCPTT group call; and

E) upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31];

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 clause 6.6.3.1.8.4:

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 3GPP TS 24.379 [29], clause F.1 with an <emergency-ind> element set to a value of "true";

c) if an <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml 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 [3] 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 clause 6.6.3.1.10 and the in-progress emergency state of the group to is set to a value of "true" the IWF performing the controlling role:

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 clause 6.6.3.1.8.3 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 MCPTT participants in the group call as specified in clause 6.6.3.1.3. The MCPTT controlling function:

i) for each of the other MCPTT participants in the group call shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [3]; and

ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31];

NOTE 3: Clause 6.6.3.1.3 will inform the group call (MCPTT) 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 clause 6.6.3.5.2;

f) for each of the affiliated MCPTT 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 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function;

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 [3];

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 clause 10.1.4.8 and skip the rest of the steps.

Upon receiving a SIP 200 (OK) response to a SIP re-INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31];

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

2) shall include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [3] with the clarifications specified in 3GPP TS 24.379 [29], clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

3) shall include the "norefersub" option tag in a Supported header field according to IETF RFC 4488 [12];

4) shall include the "tdialog" option tag in a Supported header field according to IETF RFC 4538 [13];

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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function;

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 clause 6.6.3.1.8.3, 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function;

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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function;

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 29.380 [31]; and

9) shall send the SIP 200 (OK) response towards the MCPTT client according to 3GPP TS 24.229 [3].

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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function, the IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.11.

Upon receipt of a SIP 2xx response for an outgoing SIP MESSAGE request, shall handle according to 3GPP TS 24.229 [3].

10.1.4.8 Handling of a SIP re-INVITE request for imminent peril session

This procedure is initiated by the IWF performing the controlling role as the result of an action in clause 10.1.4.7.

In the procedures in this clause:

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 IWF performing the controlling role receives a SIP re-INVITE request with an imminent peril indication set to "true", the IWF performing the controlling role:

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 IWF performing the controlling role 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 MCPTT member of the group generate a SIP MESSAGE request notification of the MCPTT user's imminent peril indication as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, 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 [3];

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 MCPTT participants in the MCPTT group call as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.15, with the IWF acting as the controlling MCPTT function;

iii) send the SIP re-INVITES to all of the other MCPTT participants in the MCPTT group call;

iv) for each of the affiliated MCPTT 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 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, 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 [3]; 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 clause 6.6.3.1.8.6 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 3GPP TS 24.379 [29], clause 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 [3]; 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 clause 6.6.3.1.8.6 and the in-progress imminent peril state of the group to is set to a value of "true" the IWF performing the controlling role 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 MCPTT participants in the MCPTT group call as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.15, with the IWF acting as the controlling MCPTT function. The MCPTT controlling function:

i) for each MCPTT participant shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [3]; and

ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the IWF performing the controlling role interact with the media plane as specified in 3GPP TS 29.380 [31]; and

NOTE 2: 3GPP TS 24.379 [29], clause 6.3.3.1.15, with the IWF acting as the controlling MCPTT function, will inform the affiliated and joined MCPTT 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 MCPTT 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 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function;

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 [3];

4) shall include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [3] with the clarifications specified in 3GPP TS 24.379 [29], clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function;

5) shall include the "norefersub" option tag in a Supported header field according to IETF RFC 4488 [12];

6) shall include the "tdialog" option tag in a Supported header field according to IETF RFC 4538 [13];

7) shall interact with media plane as specified in 3GPP TS 29.380 [31]; and

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

Upon receipt of a SIP 2xx response for an outgoing SIP MESSAGE request, shall handle according to 3GPP TS 24.229 [3].

10.1.5 Non-controlling role procedures

Editor's note: Content to be added.

10.2 Chat group (restricted) call

10.2.1 Client derived procedures

10.2.1.1 On-demand chat group call

10.2.1.1.1 Procedure for initiating an MCPTT chat group session and procedure for joining an MCPTT chat group session

This clause is referenced from other procedures.

To initiate or join an MCPTT group session using an MCPTT group identity, identifying an MCPTT chat group, the IWF performing the participating role shall generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [3], with the clarifications given below.

The IWF performing the participating role:

1) if the IWF is originating an MCPTT emergency group call shall comply with the procedures in clause 6.4.1.1;

2) if the IWF is originating an MCPTT imminent peril group call, shall comply with the procedures in clause 6.4.1.6;

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 [9];

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 [5];

5) shall include the ICSI value "urn:urn-7:3gpp-service.ims.icsi.mcptt" (coded as specified in 3GPP TS 24.229 [3]), in a P-Preferred-Service header field according to IETF RFC 6050 [7] 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 [5];

7) if the emergency group state for this group is set to "MEG 2: in-progress" or "MEG 4: confirm-pending", shall comply with the procedures in clause 6.4.1.2;

8) if the 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 clause 6.4.1.8;

9) 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 a value determined by the IWF;

NOTE 1: How the IWF determines the value of the <mcptt-client-id> element is out of scope of the present document.

NOTE 2: The <mcptt-calling-user-id> will be inserted into the body of the SIP INVITE request by the referring clause.

10) shall include an SDP offer according to 3GPP TS 24.229 [3] with the clarifications specified in clause 6.1.1;

11) if an implicit floor request is required, shall indicate this as specified in clause 6.7; and

12) shall not perform the remainder of this procedure.

On receiving a SIP 2xx response to the SIP INVITE request, the IWF performing the participating role:

1) shall interact with the media plane as specified in 3GPP TS 29.380 [31];

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", shall perform the actions specified in clause 6.4.1.4, with the IWF acting as the MCPTT client on behalf of the IWF user homed in the IWF; and

3) may subscribe to the conference event package as specified in clause 10.3.

On receiving a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request, the IWF performing the participating role:

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";

shall perform the actions specified in clause 6.4.1.5, with the IWF acting as the MCPTT client on behalf of the user homed in the IWF.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the IWF performing the participating role shall follow the actions specified in clause 6.4.1.9, with the IWF acting as the MCPTT client on behalf of the user homed in the IWF.

10.2.1.1.2 IWF performing the terminating participating role receives SIP re-INVITE request for an MCPTT chat group

This clause is referenced from other procedures.

Upon receipt of a SIP re-INVITE request the IWF performing the participating role:

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) shall set the MCPTT emergency group state to "MEG 2: in-progress";

   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";

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", 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) if the <mcpttinfo> element containing the <mcptt-Params> element contains an <alert-ind> element set to "false":

      i) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body including an <originated-by> element:

A) if the MCPTT ID contained in the <originated-by> element is the MCPTT ID associated with the targeted user, shall set the MCPTT emergency alert state to "MEA 1: no-alert";

b) shall set the MCPTT emergency group state to "MEG 1: no-emergency"; and

c) 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) 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";

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 [3];

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

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 SIP 200 (OK) response;

8) 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 [3] with the clarifications given in clause 6.1.2; and

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

10.2.1.1.3 MCPTT in-progress emergency cancel

This clause is referenced from other procedures.

To cancel an in-progress emergency state on an MCPTT chat group, the IWF performing the participating role shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [3], with the clarifications given below.

The IWF performing the participating role:

1) shall, if cancelling an in-progress emergency state and optionally an MCPTT emergency alert originated by the user homed in the IWF, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.1.3;

2) shall, if cancelling an in-progress emergency state 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 clause 6.4.1.10;

3) shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [3] with the clarifications specified in clause 6.1.1;

4) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.1.2; and

5) shall exit the procedure in the present clause.

On receiving a SIP 2xx response to the SIP re-INVITE request, the IWF performing the participating role:

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 TS 24.379 [29], clause 4.4, with the IWF acting as the MCPTT server 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 IWF performing the participating role 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: 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 IWF performing the participating role shall follow the actions specified in clause 6.4.1.9.

10.2.1.1.4 MCPTT upgrade to in-progress emergency or imminent peril

This clause is referenced from other procedures. To upgrade the MCPTT group session to an emergency condition or an imminent peril condition on a MCPTT chat group, the IWF performing the participating role shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [3], with the clarifications given below.

1) if upgrading the MCPTT group session to an MCPTT emergency call, the IWF performing the participating role:

   a) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.1.1; and

   b) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.1.2

2) if upgrading the MCPTT group session to an MCPTT imminent peril call, the IWF performing the participating role:

   a) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.1.6; and

   b) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.1.8;

3) if the SIP re-INVITE request is to be sent within an on-demand session, the IWF performing the participating role shall include in the SIP re-INVITE request an SDP offer according to 3GPP TS 24.229 [3] with the clarifications specified in clause 6.1.1;

4) if an implicit floor request is required, shall indicate this as specified in clause 6.7; and

5) shall skip the rest of the steps.

On receiving a SIP 2xx response to the SIP re-INVITE request the IWF performing the participating role:

1) shall interact with the user plane as specified in 3GPP TS 29.380 [31]; and

2) shall perform the actions specified in clause 6.4.1.4, with the IWF acting as the MCPTT client.

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request the IWF performing the participating role shall perform the actions specified in clause 6.4.1.5, with the IWF acting as the MCPTT client.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the IWF performing the participating role shall follow the actions specified in clause 6.4.1.9.

10.2.1.1.5 MCPTT in-progress imminent peril cancel

This clause is referenced from other procedures.

To cancel the in-progress imminent peril state on a MCPTT chat group, the IWF performing the participating role shall generate a SIP re-INVITE request by following the procedures specified in 3GPP TS 24.229 [3], with the clarifications given below.

The IWF performing the participating role:

1) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.1.7;

2) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.1.8;

3) 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;

4) 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 [9];

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 [3] with the clarifications specified in clause 6.1.1; and

6) shall exit the procedure in the present clause.

On receiving a SIP 2xx response to the SIP re-INVITE request, the IWF performing the participating role:

1) shall interact with the user plane as specified in 3GPP TS 29.380 [31];

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 IWF performing the participating role shall set the MCPTT imminent peril group state as "MIG 2: in-progress".

NOTE: This is the case where the IWF performing the participating role requested the cancellation of the MCPTT imminent peril in-progress state and was rejected.

10.2.1.1.6 IWF performing the terminating participating role receives a SIP INVITE request for an MCPTT chat group call

This clause is referenced from other procedures.

This procedure is used for MCPTT emergency and MCPTT imminent peril calls when the targeted client is affiliated but not joined to the chat group.

In the procedures in this clause:

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 IWF performing the participating role:

1) may reject the SIP INVITE request for any reason outside the scope of this specification;

2) if the SIP INVITE request is rejected in step 1), shall respond towards controlling MCPTT function either with appropriate reject code as specified in 3GPP TS 24.229 [3] and warning texts as specified in clause 4.2.2 or with SIP 480 (Temporarily unavailable) and skip the rest of the steps of this clause;

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) shall set the MCPTT emergency group state to "MEG 2: in-progress";

   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"; 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", shall set the MCPTT imminent peril group state to "MIG 2: in-progress";

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

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

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) shall include the Session-Expires header field in the SIP 200 (OK) response and start the SIP session timer according to IETF RFC 4028 [6]. 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;

10) 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 [3] with the clarifications given in clause 6.1.2;

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

12) shall interact with the media plane as specified in 3GPP TS 29.380 [31].

10.2.2 IWF performing the participating role procedures

10.2.2.1 On-demand chat group call

10.2.2.1.1 MCPTT chat session establishment

Editor's Note: Behaviour for cases where the IWF affiliates on behalf of users homed in the IWF is FFS.

In this clause, the IWF originates a chat group session on behalf of a user homed in the IWF.

NOTE 1: How the IWF determines the public user identity and the MCPTT ID of the calling user is out of scope of the present document.

The IWF, performing the originating participating role:

1) shall determine the public service identity of the controlling MCPTT function associated with the group identity of the group on which the call is to be originated;

NOTE 2: How the IWF discovers the public service identity of the controlling MCPTT function associated with the group identity is out of scope of the current document.

2) if the calling user identified by the MCPTT ID is not affiliated to the group on which the call is to be originated, as determined by clause 9.2.1.2.8, shall perform the actions specified in clause 9.2.1.2.9 for implicit affiliation;

3) shall generate a SIP INVITE request as specified in clause 10.2.1.1.1;

4) if step 3 was performed successfully, shall complete the SIP INVITE request as specified in clause 6.6.2.1.2;

5) if steps 3 and 4 were performed successfully:

   a) shall set the Request-URI to the public service identity of the controlling MCPTT function;

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

   c) may insert the calling user's location information into an application/vnd.3gpp.mcptt-location-info+xml MIME body;

   d) shall send the SIP INVITE request to the controlling MCPTT function as specified in 3GPP TS 24.229 [3].

Upon receipt of a SIP 302 (Moved Temporarily) response to the above SIP INVITE request, the IWF, performing the originating participating role:

1) shall generate a SIP INVITE request as specified in clause 6.6.2.1.5;

2) shall include an SDP offer based upon the SDP offer in the SIP INVITE request generated by the IWF in the step above; and

3) shall send the SIP INVITE request to the controlling MCPTT function according to 3GPP TS 24.229 [3];

Upon receipt of a SIP 2xx response to the above SIP INVITE request in step 3) the IWF performing the participating role:

1) shall perform the procedures for receiving a SIP 2xx response as specified in clause 10.2.1.1.1;

2) if the procedures of clause 9.2.1.2.9 for implicit affiliation were performed in the present clause, shall complete the implicit affiliation by performing the procedures of clause 9.2.1.2.10.

3) shall start the SIP Session timer according to rules and procedures of IETF RFC 4028 [6].

Upon receipt of a SIP 4xx, 5xx or 6xx response to the above SIP INVITE request in step 14) the IWF performing the participating role:

1) shall perform the procedures for receiving a SIP 4xx response, a SIP 5xx response or a SIP 6xx response as specified in clause 10.2.1.1.1;

2) if the implicit affiliation procedures of clause 9.2.1.2.9 were invoked in the current procedure, shall perform the procedures of clause 9.2.1.2.10.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the IWF performing the participating role shall follow the actions for SIP INFO as specified in clause 10.2.1.1.1.

10.2.2.1.2 Sending of a SIP re-INVITE request towards the MCPTT controlling function

Upon a need to send a SIP re-INVITE request for an MCPTT session identifying an on-demand MCPTT chat group session, the IWF performing the participating role:

1) if the request is for an upgrade to an in-progress emergency group state or an imminent peril group state, the IWF performing the participating role shall perform the steps in clause 10.2.1.1.4;

2) if the request is for a cancellation of an in-progress emergency group state, the IWF performing the participating role shall perform the steps in clause 10.2.1.1.3;

3) if the request is for a cancellation of an in-progress imminent peril group state, the IWF performing the participating role shall perform the steps in clause 10.2.1.1.5;

4) shall include the MCPTT ID of the originating user in the <mcptt-calling-user-id> element of the application/vnd.3gpp.mcptt-info+xml MIME body of the SIP re-INVITE request;

NOTE: How the IWF determines the MCPTT ID of a user homed in the IWF is out of scope of the present document.

5) shall include in the SIP re-INVITE request an SDP offer as specified in clause 6.6.2.1.1.1; and

6) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [3].

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

1) if the SIP re-INVITE request above is for an upgrade for emergency or imminent peril, follow the procedures for SIP 2xx response as specified in clause 10.2.1.1.4;

2) if the SIP re-INVITE request above is for an in-progress emergency cancel, follow the procedures for SIP 2xx response as specified in clause 10.2.1.1.3; or

3) if the SIP re-INVITE request above is for an in-progress imminent peril cancel, follow the procedures for SIP 2xx response as specified in clause 10.2.1.1.5.

Upon receipt of a SIP 403 (Forbidden) response to the sent SIP re-INVITE request the participating MCPTT function, the IWF action is out of scope of the present document.

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request the IWF:

1) if the SIP re-INVITE request above is for an upgrade for emergency or imminent peril, follow the procedures for SIP 4xx, 5xx or 6xx response as specified in clause 10.2.1.1.4;

2) if the SIP re-INVITE request above is for an in-progress emergency cancel, follow the procedures for SIP 4xx, 5xx or 6xx response as specified in clause 10.2.1.1.3; or

3) if the SIP re-INVITE request above is for an in-progress imminent peril cancel, follow the procedures for SIP 4xx, 5xx or 6xx response as specified in clause 10.2.1.1.5.

Upon receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing session, the IWF performing the participating role shall:

1) if the SIP re-INVITE request above is for an upgrade for emergency or imminent peril, follow the procedures for SIP INFO as specified in clause 10.2.1.1.4; or

2) if the SIP re-INVITE request above is for an in-progress emergency cancel, follow the procedures for SIP INFO as specified in clause 10.2.1.1.3.

10.2.2.1.3 Reception of a SIP INVITE request by an IWF performing the terminating participating role

Upon receipt of a "SIP INVITE request for terminating participating MCPTT function", targeting a user homed in the IWF for an MCPTT chat group, the IWF performing the participating role:

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 IWF performing the participating role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14]. Otherwise, continue with the rest of the steps;

2) shall check the presence of the isfocus media feature tag in the Contact header field and if it is not present then the IWF performing the participating role 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 clause 4.4. Otherwise, continue with the rest of the steps; and

3) shall perform the steps in 10.2.1.1.6.

10.2.2.1.4 Reception of a SIP re-INVITE request by an IWF performing the terminating participating role

Upon receipt of a SIP re-INVITE targeting a user homed in the IWF for an MCPTT chat group, the IWF performing the participating role shall perform the steps in 10.2.1.1.2.

10.2.2.2 End group call at the originating participating IWF

10.2.2.2.1 IWF ending on-demand chat session

When the IWF performing the participating role determines a need to send a SIP BYE request, the IWF shall follow the procedures as specified in clause 6.6.2.1.3.

10.2.2.3 End group call at the terminating participating IWF

10.2.2.3.1 Receipt of SIP BYE request for on-demand chat session

Upon receiving a SIP BYE request from the controlling MCPTT function, the IWF performing the participating role shall follow the procedures as specified in clause 6.6.2.2.2.1.

10.2.3 IWF controlling role procedures

10.2.3.1 On-demand chat group call

10.2.3.1.1 Procedure for establishing an MCPTT chat session and procedure for joining an established MCPTT chat session

In the procedures in this clause:

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 MCPTT chat group, the IWF performing the controlling role:

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 IWF performing the controlling role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14] 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 IWF performing the controlling role 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.mcptt-info+xml MIME body with an <emergency-ind> element included or an <imminentperil-ind> element included, shall validate the request as described in 3GPP TS 24.379 [29], clause 6.3.3.1.17, with the IWF acting as the controlling MCPTT function;

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 3GPP TS 24.379 [29], clause 6.3.5.2, with the IWF acting as the participating MCPTT function and continue with the rest of the steps if the checks in 3GPP TS 24.379 [29], clause 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 3GPP TS 24.379 [29], clause 6.3.6, with the IWF acting as the controlling MCPTT function:

   a) shall check if the MCPTT user is eligible to be implicitly affiliated with the MCPTT chat group as determined by clause 9.2.1.3.6; 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function 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 clause 6.6.3.1.8.2:

   a) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response as specified in clause 6.6.3.1.9; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [3] 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 clause 6.6.3.1.8.6, 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 3GPP TS 24.379 [29], 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 [3] 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 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 IWF performing the controlling role 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 clause 6.6.3.5;

11) if the chat group session is ongoing and the <on-network-max-participant-count> as specified in 3GPP TS 24.481 [16] 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 clause 10.1.4.4.3, 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 [16]. 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function. 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 clause 9.2.1.3.7 was not previously invoked in the present clause, shall perform the implicit affiliation as specified in clause 9.2.1.3.7;

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 IWF performing the controlling role 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 clause 6.6.3.1.12, and if not:

i) perform the actions specified in clause 6.6.3.1.5;

ii) send the SIP UPDATE request generated in clause 6.6.3.1.5 towards the initiator of the SIP INVITE request according to 3GPP TS 24.229 [3]; and

iii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in clause 6.6.3.1.5, 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 MCPTT members of the group generate a SIP MESSAGE request notification of the MCPTT user's emergency indication as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, 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 clause 6.6.3.1.8.1, perform the procedures specified in clause 6.6.3.1.7; and

C) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [3];

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 clause 6.6.3.1.10;

iii) shall generate SIP re-INVITE requests for the MCPTT emergency group call to the other MCPTT affiliated and joined participants of the MCPTT chat group as specified in clause 6.6.3.1.3;

iv) shall generate SIP INVITE requests for the MCPTT emergency group call to the affiliated but not joined MCPTT members of the MCPTT chat group as specified in clause 6.6.3.1.4;

A) for each affiliated but not joined MCPTT member shall send the SIP INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [3]; and

B) upon receiving a SIP 200 (OK) response to the SIP INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31];

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 clause 6.6.3.1.8.1, 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 IWF performing the controlling role 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 clause 6.6.3.1.12, and if not:

i) perform the actions specified in clause 6.6.3.1.5;

ii) send the SIP UPDATE request generated in clause 6.6.3.1.5 towards the initiator of the SIP INVITE request according to 3GPP TS 24.229 [3]; and

iii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in clause 6.6.3.1.5 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 MCPTT member of the group generate a SIP MESSAGE request notification of the MCPTT user's imminent peril indication as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, 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 [3]; 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 MCPTT affiliated and joined participants of the MCPTT chat group as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.15, with the IWF acting as the controlling MCPTT function;

iii) shall generate SIP INVITE requests for the MCPTT imminent peril call to the affiliated but not joined MCPTT members of the MCPTT chat group as specified in clause 6.6.3.1.4;

A) for each affiliated but not joined MCPTT member shall send the SIP INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [3]; and

B) Upon receiving a SIP 200 (OK) response to the SIP INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31]; 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 [3];

16) shall include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [3] with the clarifications specified in 3GPP TS 24.379 [29], clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function, unless the procedures of clause 6.6.3.1.5 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 [6]. 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 [13];

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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function;

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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function;

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 29.380 [31];

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

25) if the chat group session was already ongoing and if at least one of the MCPTT participants has subscribed to the conference event package, shall send a SIP NOTIFY request to all MCPTT participants with a subscription to the conference event package as specified in 3GPP TS 24.379 [29], clause 10.1.3.4.2 with the IWF acting as the controlling MCPTT function.

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 clause 4.4, the IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.11.

10.2.3.1.2 Receipt of a SIP re-INVITE request

In the procedures in this clause:

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 MCPTT chat group session, the IWF performing the controlling role:

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 IWF performing the controlling role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14] 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 clause 6.6.3.1.8.2, or for originating an MCPTT imminent peril group call as determined by clause 6.6.3.1.8.5, the IWF performing the controlling role 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 3GPP TS 24.379 [29], clause 6.3.3.1.17, with the IWF acting as the controlling MCPTT function;

3) if the SIP re-INVITE request contains an unauthorised request for an MCPTT emergency call as determined by clause 6.6.3.1.8.2:

   a) shall reject the SIP re-INVITE request with a SIP 403 (Forbidden) response as specified in clause 6.6.3.1.9; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [3] 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 clause 6.6.3.1.8.2, the IWF performing the controlling role 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 clause 6.6.3.1.12, and if not:

      i) shall perform the actions specified in clause 6.6.3.1.5; and

      ii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in clause 6.6.3.1.5 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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, 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 clause 6.6.3.1.8.1, perform the procedures specified in clause 6.6.3.1.7; and

         C) send the SIP MESSAGE request as specified in 3GPP TS 24.229 [3]; 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 clause 6.6.3.1.8.1, 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 clause 6.6.3.1.10;

v) shall generate SIP re-INVITE requests for the MCPTT emergency group call to the other affiliated and joined participants of the MCPTT chat group as specified in clause 6.6.3.1.3. The IWF performing the controlling role:

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 [3]; and

B) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

vi) shall generate SIP INVITE requests for the MCPTT emergency group call to the affiliated but not joined MCPTT members of the MCPTT chat group as specified in clause 6.6.3.1.4. The IWF performing the controlling role:

A) for each affiliated but not joined MCPTT member shall send the SIP INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [3]; and

B) Upon receiving a SIP 200 (OK) response to the SIP INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31]; 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 clause 6.6.3.1.8.4:

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 3GPP TS 24.379 [29], clause F.1 with an <emergency-ind> element set to a value of "true";

c) if an <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml 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 [3] 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 clause 6.6.3.1.8.4 and the in-progress emergency state of the group to is set to a value of "true" the IWF performing the controlling role 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 clause 6.6.3.1.12, and if not:

i) shall perform the actions specified in clause 6.6.3.1.5; and

ii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in clause 6.6.3.1.5 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) set the in-progress emergency group state of the group to a value of "false";

c) 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 clause 6.6.3.1.8.3 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) generate SIP re-INVITE requests to the other affiliated and joined members of the MCPTT group as specified in clause 6.6.3.1.3. The IWF performing the controlling role:

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 [3]; and

ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

NOTE 4: Clause 6.6.3.1.3 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 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function;

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 [3];

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 clause 6.6.3.1.8.5 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 clause 10.2.3.1.3 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 [3] with the clarifications specified in 3GPP TS 24.379 [29], clause 6.3.3.2.1, with the IWF acting as the controlling MCPTT function, unless the procedures of clause 6.6.3.1.5 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 [13];

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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function;

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 clause 6.6.3.1.8.3, 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function;

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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function;

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 29.380 [31]; and

15) shall send the SIP 200 (OK) response towards the MCPTT client according to 3GPP TS 24.229 [3].

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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling MCPTT function, the IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.11.

10.2.3.1.3 Handling of a SIP re-INVITE request for imminent peril session

In the procedures in this clause:

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 IWF performing the controlling role receives a SIP re-INVITE request with and imminent peril indication, the IWF performing the controlling role:

1) if the SIP re-INVITE request contains an unauthorised request for an MCPTT imminent peril group call as determined by clause 6.6.3.1.8.5, 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 3GPP TS 24.379 [29], 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 [3] 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 IWF performing the controlling role 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 [23] and the priority set to the priority designated for imminent peril calls and if not:

      i) perform the actions specified in clause 6.6.3.1.5;

      ii) send the SIP UPDATE request generated in clause 6.6.3.1.5 towards the initiator of the SIP re-INVITE request according to 3GPP TS 24.229 [3]; and

      iii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in clause 6.6.3.1.5 proceed with the rest of the steps.

NOTE 1: 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 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling function, 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 [3]; 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 MCPTT chat group as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.15, with the IWF acting as the controlling MCPTT function;

iii) shall generate SIP INVITE requests for the MCPTT imminent peril group call to the affiliated but not joined members of the MCPTT chat group as specified in clause 6.6.3.1.4;

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 [3]; and

B) Upon receiving a SIP 200 (OK) response to the SIP INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31]; 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 clause 6.6.3.1.8.6 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 3GPP TS 24.379 [29], clause 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 [3]; 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 clause 6.6.3.1.8.6 and the in-progress imminent peril state of the group to is set to a value of "true" the IWF performing the controlling role 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 [23], and the priority set to the priority level designated for a normal priority MCPTT group call, and if not:

i) perform the actions specified in clause 6.6.3.1.5; and

ii) upon receiving a SIP 200 (OK) response to the SIP UPDATE request sent in clause 6.6.3.1.5, proceed with the rest of the steps;

NOTE 2: verify that the Resource-Priority header is included and properly populated for an in-progress emergency group state cancellation of the specified group.

b) set the in-progress imminent peril state of the group to a value of "false";

c) cache the information that the MCPTT user no longer has an outstanding MCPTT imminent peril group call;

d) generate SIP re-INVITES requests to the other affiliated and joined members of the MCPTT group as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.15, with the IWF acting as the controlling MCPTT function. The IWF performing the controlling role:

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 [3]; and

ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request the IWF performing the controlling role shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

NOTE 3: 3GPP TS 24.379 [29], clause 6.3.3.1.15, with the IWF acting as the controlling MCPTT function, 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 MCPTT members of the group:

i) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's imminent peril call as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function;

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 [3];

5) include in the SIP 200 (OK) response an SDP answer according to 3GPP TS 24.229 [3] with the clarifications specified in 3GPP TS 24.379 [29], clause 6.3.3.2.1 unless the procedures of clause 6.6.3.1.5 were performed in step 2) or 4) above;

6) include the "norefersub" option tag in a Supported header field according to IETF RFC 4488 [12];

7) include the "tdialog" option tag in a Supported header field according to IETF RFC 4538 [13];

8) interact with media plane as specified in 3GPP TS 29.380 [31]; and

9) send the SIP 200 (OK) response towards the MCPTT client according to 3GPP TS 24.229 [3].

10.2.3.2 End group call at the terminating IWF performing the controlling role

Upon receiving a SIP BYE request the IWF performing the controlling role shall follow the procedures as specified in clause 6.6.3.2.1.

10.2.3.3 End group call initiated by the IWF performing the controlling role

10.2.3.3.1 General

This clause describes the procedures of each functional entity for ending the group call initiated by the IWF performing the controlling role.

10.2.3.3.2 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 clause 6.6.7.1, the IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.2.

10.2.3.3.3 SIP BYE request towards 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 IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.2.

After successfully removing the MCPTT client from the MCPTT session, the IWF performing the controlling role may generate a notification to the MCPTT clients, which have subscribed to the conference event package that an MCPTT

user has been removed from the MCPTT session, as specified in clause 6.6.3.4 and send the SIP NOTIFY request to the MCPTT client according to 3GPP TS 24.229 [3].

10.2.3.3.4 Removal of participant homed in the IWF

After successfully removing a participant homed in the IWF from the MCPTT session, the IWF performing the controlling role may generate a notification to any MCPTT clients in the session, which have subscribed to the conference event package that a user has been removed from the MCPTT session, as specified in clause 6.6.3.4 and send the SIP NOTIFY request to the MCPTT client according to 3GPP TS 24.229 [3].

10.2.4 Non-controlling role procedures

Editor's note: Content to be added.

10.3 Subscription to the conference event package

Editor's note: Content to be added.

10.4 Remotely initiated group call

10.4.1 Participating MCPTT function procedures

10.4.1.1 IWF performing the participating role

10.4.1.1.1 Originating procedures

Originating procedures are not supported in this version of the specification.

10.4.1.1.2 Terminating procedures

Upon receiving a "SIP MESSAGE request for remotely initiated group call for terminating participating function" the IWF performing the participating role shall reject the SIP MESSAGE request with a SIP 501 (Not Implemented) response.

10.4.1.2 IWF performing the controlling role

Upon receiving:

- a "SIP MESSAGE request for remotely initiated group call request for controlling MCPTT function"; or
- a "SIP MESSAGE request for remotely initiated group call response for controlling MCPTT function";

the IWF performing the controlling role shall reject the SIP MESSAGE request with a SIP 501 (Not Implemented) response.

11 Private call call control

11.1 Private call with floor control

11.1.1 Client derived procedures

11.1.1.1 On-demand private call

11.1.1.1.1 Originating procedures

This clause is referenced from other procedures.

To establish an MCPTT private call the IWF performing the participating role shall generate an initial SIP INVITE request by following the UE originating session procedures specified in 3GPP TS 24.229 [3], with the clarifications given below.

The IWF performing the participating role:

1) if originating an MCPTT emergency private call or originating an MCPTT private call and the MCPTT emergency state is already set, the IWF performing the participating role, shall comply with the procedures in clause 6.4.2.1;

2) 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 [9];

3) 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 [5];

4) 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 [5];

5) 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 [11];

6) if a security context needs to be established between the IWF and the MCPTT client and if the user homed in the IWF is initiating a private call then:

   a) if necessary, request keying material from the key management server as described in 3GPP TS 33.180 [27];

   b) shall use the keying material to generate a PCK as described in 3GPP TS 33.180 [27];

   c) shall use the PCK to generate a PCK-ID with the four most significant bits set to "0000" 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 [27];

   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 [27];

NOTE 1: How the IWF obtains the KMS URI of the invited user is out of scope of the present document.

   e) shall generate a MIKEY-SAKKE I_MESSAGE using the encapsulated PCK and PCK-ID as specified in 3GPP TS 33.180 [27]; and

   f) shall add the MCPTT ID of the originating user homed in the IWF to the initiator field (IDRi) of the I_MESSAGE as described in 3GPP TS 33.180 [27]; and

   g) shall sign the MIKEY-SAKKE I_MESSAGE using the originating user homed in the IWF'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 [27];

7) shall include an SDP offer according to 3GPP TS 24.229 [3] with the clarification given in clause 6.1.1 and with a media stream of the offered media-floor control entity;

8) if implicit floor control is required, shall comply with the conditions specified in clause 6.7;

9) if force of automatic commencement mode at the invited MCPTT client is requested by the user homed in the IWF, 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 [10];

10) if force of automatic commencement mode at the invited MCPTT client is not requested by the user homed in the IWF:

   a) if automatic commencement mode at the invited MCPTT client is requested by the user homed in the IWF, 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 [10]; and

   b) if manual commencement mode at the invited MCPTT client is requested by the user homed in the IWF, 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 [10]; and

11) 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"; and

12) if the MCPTT emergency private call state of the user homed in the IWF 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 IWF shall comply with the procedures in clause 6.4.2.2.

NOTE 2: Upon receiving a SIP 183(Session Progress) response to the SIP INVITE request the IWF performing the participating role's actions are out of scope of the present document.

Upon receiving a SIP 200 (OK) response to the SIP INVITE request the IWF performing the participating role:

1) shall interact with the media plane as specified in 3GPP TS 29.380 [31];

2) 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 3GPP TS 24.379 [29], clause 6.2.8.3.4, with the IWF acting as the MCPTT client on behalf of the IWF user homed in the IWF; and

3) shall consider the call 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 IWF performing the participating role shall perform the actions specified in 3GPP TS 24.379 [29], clause 6.2.8.3.5, with the IWF acting as the MCPTT client on behalf of the IWF user homed in the IWF.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing session, the IWF performing the participating role shall follow the actions specified in 3GPP TS 24.379 [29], clause 6.2.8.3.7 with the IWF acting as the MCPTT client on behalf of the IWF user homed in the IWF.

11.1.1.1.2 IWF terminating procedures

This clause is referenced from other procedures.

The IWF performing the participating role:

1) may reject the SIP INVITE request for any other reason outside the scope of this specification otherwise, continue with the rest of the steps.

2) if the SIP INVITE request is rejected in step 1), shall respond towards the controlling MCPTT function either with appropriate reject code as specified in 3GPP TS 24.229 [3] and warning texts as specified in clause 4.2.2 or with SIP 480 (Temporarily unavailable) response and skip the rest of the steps of this clause;

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":

   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 [27];

   b) shall convert the MCPTT ID to a UID as described in 3GPP TS 33.180 [27];

   c) shall use the UID to validate the signature of the MIKEY-SAKKE I_MESSAGE as described in 3GPP TS 33.180 [27];

   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 [22], and include warning text set to "136 authentication of the MIKEY-SAKE I_MESSAGE failed" in a Warning header field as specified in clause 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 [27]; and

      ii) shall extract the PCK-ID, from the payload as specified in 3GPP TS 33.180 [27];

NOTE: With the PCK successfully shared between the originating and the terminating parties, the IWF and the MCPTT client are able to use SRTP/SRTCP to create a secure session.

5) shall perform the automatic commencement procedures specified in clause 6.2.1 if one of the following conditions are met:

   a) SIP INVITE request contains an Answer-Mode header field with the value "Auto" and the IWF is configured for automatic commencement mode for the user receiving the call;

   c) SIP INVITE request contains a Priv-Answer-Mode header field with the value of "Auto" and the IWF is able to process an automatic commencement; and

6) shall perform the manual commencement procedures specified in clause 6.2.2 if either of the following conditions are met:

   a) SIP INVITE request contains an Answer-Mode header field with the value "Manual" and the IWF is configured for manual commencement mode for the user receiving the call;

   b) SIP INVITE request contains a Priv-Answer-Mode header field with the value of "Manual" and the IWF is able to process a manual commencement.

Upon receiving the SIP CANCEL request cancelling a SIP INVITE request for which a dialog exists at the IWF performing the participating role and a SIP 200 (OK) response has not yet been sent to the SIP INVITE request then the IWF performing the participating role:

1) shall send a SIP 200 (OK) response to the SIP CANCEL request according to 3GPP TS 24.229 [3]; and

2) shall send a SIP 487 (Request Terminated) response to the SIP INVITE request according to 3GPP TS 24.229 [3].

Upon receiving a SIP BYE request for an established dialog, the IWF performing the participating role:

1) shall follow the procedures in clause 11.4.1.1.

11.1.1.1.3 Terminating procedures for reception of SIP re-INVITE request

This clause is referenced from other procedures.

Upon receipt of a SIP re-INVITE request for an existing private call session, the IWF performing the participating role 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":

   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) if the SIP re-INVITE request contains an application/vnd.3gpp.mcptt-info+xml MIME body including an <originated-by> element:

      i) 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 [3]; and

NOTE: 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.

4) 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 [3] with the clarifications given in clause 6.1.2 with the IWF acting as the MCPTT client.

11.1.1.1.4 MCPTT in-progress emergency cancel

This clause is referenced from other procedures.

To cancel the in-progress emergency condition on an MCPTT emergency private call, the IWF performing the participating role shall generate a SIP re-INVITE request by following the UE session procedures specified in 3GPP TS 24.229 [3], with the clarifications given below.

The IWF performing the participating role:

1) shall, if cancelling an in-progress emergency condition and optionally an MCPTT emergency alert originated for the user homed in the IWF, include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.2.3;

2) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.2.2;

3) shall include in the SIP re-INVITE request an SDP offer with the media parameters as currently established;

4) if an implicit floor request is required, shall indicate this as specified in clause 6.7; and

5) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [3].

On receiving a SIP 2xx response to the SIP re-INVITE request, the IWF performing the participating role:

1) shall interact with the user plane as specified in 3GPP TS 29.380 [31];

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 3GPP TS 24.379 [29], clause 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 IWF performing the participating role 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 IWF performing the participating role 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, the IWF performing the participating role 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: 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 IWF performing the participating role shall follow the actions specified in 3GPP TS 24.379 [29], clause 6.2.8.3.7 with the IWF acting as the MCPTT client.

11.1.1.1.5 Upgrade to MCPTT emergency private call

This clause is referenced by other clauses.

To upgrade the ongoing MCPTT private call to an MCPTT emergency private call, the IWF performing the participating role shall generate a SIP re-INVITE request as specified in 3GPP TS 24.229 [3], with the clarifications given below.

1) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.2.1;

2) shall include a Resource-Priority header field and comply with the procedures in clause 6.4.2.2.

3) shall include an SDP offer with the media parameters as currently established according to 3GPP TS 24.229 [3];

4) if an implicit floor request is required, shall indicate this as specified in clause 6.7; and

5) shall send the SIP re-INVITE request according to 3GPP TS 24.229 [3].

On receiving a SIP 2xx response to the SIP re-INVITE request the IWF performing the participating role:

1) shall interact with the user plane as specified in 3GPP TS 29.380 [31]; and

2) shall perform the actions specified in 3GPP TS 24.379 [29], clause 6.2.8.3.4 with the IWF acting as the MCPTT client.

On receiving a SIP 4xx response, SIP 5xx response or SIP 6xx response to the SIP re-INVITE request, the IWF performing the participating role shall perform the actions specified in 3GPP TS 24.379 [29], clause 6.2.8.3.5 with the IWF acting as MCPTT client.

On receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing group session, the IWF performing the participating role shall follow the actions specified in 3GPP TS 24.379 [29], clause 6.2.8.3.7 with the IWF acting as the MCPTT client.

11.1.2 IWF participating role procedures

11.1.2.1 Originating procedures

11.1.2.1.1 On-demand private call

In the present clause, the IWF performing the participating role initiates an on-demand private call. The IWF performing the participating role:

1) shall determine the MCPTT ID of the calling user;

NOTE: How the IWF determines the MCPTT ID of a user homed in the IWF is out of scope of the present document.

2) shall determine the public service identity of the controlling MCPTT function for the private call service associated with the originating user's MCPTT ID identity;

3) shall generate a SIP INVITE request as specified in clause 11.1.1.1.1;

4) shall modify the SIP INVITE as specified in clause 6.6.2.1.2;

5) shall set the Request-URI to the public service identity of the controlling MCPTT function hosting the private call service as determined by step 3;

6) 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;

7) if the SIP INVITE request contains an emergency indication set to a value of "true", may include a Resource-Priority header field populated with the values for an emergency call as specified in clause 6.4.1.11; otherwise, may include a Resource-Priority header field populated with the values for a normal call as specified in clause 6.4.1.11; and

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

Upon receiving a SIP 180 (Ringing) response, the IWF performing the participating role's action are out of scope of the present document.

Upon receiving a SIP 200 (OK) response, the IWF performing the participating role:

1) shall perform the procedures for receiving a SIP 200 ok as specified in clause 11.1.1.1.1; and

2) shall start the SIP session timer according to rules and procedures of IETF RFC 4028 [6].

On receiving a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request, the IWF performing the participating role shall follow the procedures for SIP 4xx, SIP 5xx and SIP 6xx responses as specified in clause 11.1.1.1.1.

Upon receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing session, the IWF performing the participating role shall follow the procedures for SIP INFO as specified in clause 11.1.1.1.1.

11.1.2.1.2 SIP re-INVITE for MCPTT private call

Upon deciding to send a SIP re-INVITE for an existing private call session, the IWF performing the participating role:

1) shall determine the MCPTT ID of the calling user;

NOTE 1: How the IWF determines the MCPTT ID of a user homed in the IWF is out of scope of the present document.

2) if the SIP re-INVITE is to upgrade the call to an emergency call, shall generate a SIP re-INVITE request as specified in clause 11.1.1.1.5;

3) if the SIP re-INVITE is to cancel the emergency on the call, shall generate a SIP re-INVITE request as specified in clause 11.1.1.1.4;

4) 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 homed in the IWF;

NOTE 2: How the IWF determines the MCPTT ID of a user homed in the IWF is out of scope of the present document.

5) shall, if the SIP re-INVITE is to be sent within an on-demand session include in the SIP re-INVITE request an SDP containing the current media parameters used by the existing session;

6) shall include a Resource-Priority header field as specified in clause 6.4.1.11; and

7) shall forward the SIP re-INVITE request, according to 3GPP TS 24.229 [3].

Upon receiving a SIP 200 (OK) response, the IWF performing the participating role:

1) shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

2) shall follow the procedures for SIP 200 (OK) response as specified in clause 11.1.1.1.4 if an emergency is being cancelled in the present clause or as specified in clause 11.1.1.1.5 if the call is being upgraded to emergency in the present clause. The IWF performing the participating role 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 [3].

On receiving a SIP 4xx response, a SIP 5xx response or a SIP 6xx response to the SIP INVITE request, the IWF performing the participating role shall follow the procedures for SIP 4xx, SIP5xx and SIP 6xx responses as specified in clause 11.1.1.1.4 if an emergency is being cancelled in the present clause or as specified in clause 11.1.1.1.5 if the call is being upgraded to emergency in the present clause.

Upon receiving a SIP INFO request where the Request-URI contains an MCPTT session ID identifying an ongoing session, the IWF performing the participating role shall follow the procedures for SIP INFO as specified in clause 11.1.1.1.4 if an emergency is being cancelled in the present clause or as specified in clause 11.1.1.1.5 if the call is being upgraded to emergency in the present clause.

11.1.2.2 Terminating procedures

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

1) shall respond with a SIP 488 (not acceptable here) with a body part as described in clause 6.10.2 if the IWF does not support one or more parameters of the call as described in clause 6.10.1;

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 terminating participating MCPTT function" with a SIP 500 (Server Internal Error) response. The IWF may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14], 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 IWF can choose to accept the request.

3) 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 IWF 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 3GPP TS 24.379 [29], clause 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; and

5) the IWF may 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 3GPP TS 24.379 [29], clause 4.4.

The IWF performing the participating role sends the SIP 200 (OK) response to the originating network:

1) shall generate a SIP 200 (OK) response as described in 3GPP TS 24.379 [29], clause 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 3GPP TS 24.379 [29], clause 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 29.380 [31] clause 6.4; and

5) shall forward the SIP 200 (OK) response according to 3GPP TS 24.229 [3].

11.1.2.3 Receipt of SIP re-INVITE request by terminating participating function

This clause covers the on-demand session case only.

Upon receipt of a SIP re-INVITE request for an existing MCPTT private call session the IWF performing the participating role:

1) if unable to process the request due to a lack of resources or a risk of congestion exists, shall reject the SIP re-INVITE with a SIP 500 (Server Internal Error) response. The IWF performing the participating role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14] and shall skip the rest of the steps;

NOTE 1: If the SIP re-INVITE request contains an emergency indication, the IWF performing the participating role can choose to accept the request.

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.

2) shall generate a SIP 200 (OK) response as described in 3GPP TS 24.379 [29], clause 6.3.2.2.4.2, with the IWF acting as the participating MCPTT function;

3) shall perform the procedures in clause 11.1.1.1.3;

4) shall modify the SDP answer in the received SIP 200 (OK) response as specified in 3GPP TS 24.379 [29], clause 6.3.2.2.2.1 with the IWF acting as the participating function;

5) shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

6) shall forward the SIP 200 (OK) response according to 3GPP TS 24.229 [3].

11.1.3 IWF controlling role procedures

11.1.3.1 Originating procedures

This clause describes the procedures for inviting an MCPTT user to an MCPTT session. The procedure is initiated by the IWF performing the controlling role.

The IWF performing the controlling role:

1) shall generate a SIP INVITE request as specified in clause 6.6.3.1.1;

2) shall set the <mcptt-calling-user-id> to the calling user's MCPTT ID in the outgoing SIP INVITE;

3) if the received request is for an MCPTT emergency private call as determined by clause 6.6.3.1.8.2:

   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 request is for an MCPTT emergency alert, shall perform the procedures specified in clause 6.6.3.1.7; and

c) if the request is not for an MCPTT emergency alert, shall set the <alert-ind> element of the application/vnd.3gpp.mcptt-info+xml MIME body to a value of "false";

4) shall copy the MCPTT ID of the called MCPTT user 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 1: How the IWF performing the controlling role finds the address of the terminating MCPTT participating function is out of the scope of the current release.

NOTE 2: The terminating MCPTT user is part of a partner MCPTT system, therefore 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 include a Resource-Priority header field populated with the values for an MCPTT emergency private call as specified in clause 6.6.3.1.12, if either of the following conditions is met:

a) if the request is for an MCPTT emergency private call as determined in step 2 above; or

b) the originating user homed in the IWF is in an in-progress emergency private call state with the targeted MCPTT user;

7) shall include an SDP offer according to 3GPP TS 24.229 [3] with the clarification given in clause 6.1.1 and with a media stream of the offered media-floor control entity and according to the procedures specified in 3GPP TS 24.379 [29], clause 6.3.3.1.1 with the IWF acting as the controlling MCPTT function;

8) shall send the SIP INVITE request towards the core network according to 3GPP TS 24.229 [3]; 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 IWF performing the controlling role:

1) shall cache the contact received in the Contact header field; and

2) shall interact with the media plane as specified in 3GPP TS 29.380 [31].

Upon expiry of the private call timer, the IWF performing the controlling role shall follow the procedure for releasing private call session as specified in clause 11.4.3.

11.1.3.2 Terminating procedures

In the procedures in this clause:

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", the IWF performing the controlling role:

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 clause 6.6.6.1 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 IWF performing the controlling role 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 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 3GPP TS 24.379 [29], clause 4.4, and shall not continue with the rest of the steps;

3) 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 controlling MCPTT function of a private call" 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 3GPP TS 24.379 [29], clause 4.4, and shall not continue with 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 IWF performing the controlling role and if not, reject the request with a SIP 488 (Not Acceptable Here) response and skip the rest of the steps;

5) if received SIP INVITE request includes an <emergency-ind>, shall validate the request as described in 3GPP TS 24.379 [29], clause 6.3.3.1.17, with the IWF acting as the controlling function;

6) if the received SIP INVITE request contains an unauthorised request for an MCPTT emergency private call as determined by clause 6.6.3.1.8.2:

   a) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response as specified in clause 6.6.3.1.9; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [3] and skip the rest of the steps;

7) 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;

8) 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 user homed in the IWF; 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 user homed in the IWF;

9) shall perform actions as described in 3GPP TS 24.379 [29], clause 6.3.3.2.2, with the IWF acting as the controlling MCPTT function;

10) shall allocate an MCPTT session identity for the MCPTT session; and

11) shall set up a private call with the targeted user homed in the IWF (the user whose MCPTT ID is listed in the MIME resource-lists body of received SIP INVITE request).

NOTE 1: How the IWF sets up calls internally is out of scope of the present document.

Upon deciding to send 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 IWF performing the controlling role 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 [3].

Upon deciding to accept the call, the IWF performing the controlling role:

1) shall generate a SIP 200 (OK) response to the SIP INVITE request as specified in the 3GPP TS 24.379 [29] clause 6.3.3.2.3.2, with the IWF acting as the MCPTT controlling function, 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 3GPP TS 24.379 [29] clause 6.3.3.2.2, with the IWF acting as the controlling MCPTT function;

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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling function;

NOTE 2: 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 29.380 [31]; and

NOTE 3: 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 [3].

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 3GPP TS 24.379 [29], clause 4.4, with the IWF acting as the controlling function with the warning text containing the mcptt-warn-code set to "149", the IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.11.

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 IWF performing the controlling role shall follow the procedures in clause 6.6.3.2.1.

11.1.3.3 Receiving a SIP re-INVITE for upgrade to emergency private call

In the procedures in this clause:

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 IWF performing the controlling role:

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 IWF performing the controlling role 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 3GPP TS 24.379 [29], clause 6.3.3.1.17 with the IWF acting as the MCPTT server;

3) if the SIP re-INVITE request contains an unauthorised request for an MCPTT emergency private call as determined by clause 6.6.3.1.8.2:

   a) shall reject the SIP INVITE request with a SIP 403 (Forbidden) response as specified in clause 6.6.3.1.9; and

   b) shall send the SIP 403 (Forbidden) response as specified in 3GPP TS 24.229 [3] and skip the rest of the steps;

4) 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 user:

   a) shall cache the information that the MCPTT user is in an in-progress emergency private call state with the targeted user; and

b) if the SIP re-INVITE request contains an alert indication set to "true", shall cache the information that the MCPTT user has sent an MCPTT emergency alert to the targeted user; and

5) shall perform the steps in clause 11.1.2.3 with the IWF performing the participating role but shall not forward the SIP 200 (OK) response.

If the SIP response has not yet been sent towards the inviting MCPTT client, the IWF performing the controlling role:

1) shall modify the SIP 200 (OK) response to the SIP re-INVITE request as specified in 3GPP TS 24.379 [29], clause 6.3.3.2.3.2 with the IWF acting as the controlling function before continuing with the rest of the steps;

2) 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 clause 6.6.3.1.8.1, 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 3GPP TS 24.379 [29], clause 4.4 with the IWF acting as the MCPTT server.

NOTE: When a SIP 200 (OK) response sent towards 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 IWF performing the controlling role.

3) shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

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

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 3GPP TS 24.379 [29], clause 4.4 with the IWF acting as the MCPTT server, the IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.11.

11.1.3.4 Receiving a SIP re-INVITE for cancellation of emergency private call

In the procedures in this clause:

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 IWF performing the controlling role:

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 IWF performing the controlling role 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 3GPP TS 24.379 [29], clause 6.3.3.1.17 with the IWF acting as the controlling function;

3) if the SIP re-INVITE request contains an unauthorised request for an MCPTT emergency private call cancellation as determined by local policy:

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 3GPP TS 24.379 [29], clause 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 determined by local policy, 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 [3] and skip the rest of the steps;

4) if the SIP re-INVITE request contains an authorised request for an MCPTT emergency private call cancellation as determined by clause 6.6.3.1.8.4:

   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 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 clause 6.6.3.1.8.3:

      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 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; and

5) shall perform the steps in clause 11.1.2.3 but shall not forward the SIP 200 (OK) response.

If the SIP response has not yet been sent towards the inviting MCPTT client, the IWF performing the controlling role:

1) shall modify the SIP 200 (OK) response to the SIP re-INVITE request as specified in 3GPP TS 24.379 [29], clause 6.3.3.2.3.2 with the IWF acting as the controlling function before continuing with the rest of the steps;

2) 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 clause 6.6.3.1.8.3, 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 3GPP TS 24.379 [29], clause 4.4 with the IWF acting as the MCPTT server.

NOTE: When a SIP 200 (OK) response sent towards 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 IWF performing the controlling role.

3) shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

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

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 3GPP TS 24.379 [29], clause 4.4 with the IWF acting as the MCPTT server, with the IWF acting as the controlling function shall follow the procedures in clause 6.6.3.1.11.

11.1.3.5 Sending a SIP re-INVITE for upgrade to emergency private call

This clause 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 IWF performing the controlling role.

The IWF performing the controlling role:

1) shall generate a SIP re-INVITE request as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.9, with the IWF acting as the controlling function;

2) if the originating user homed in the IWF is not in an in-progress emergency private call state with the targeted MCPTT user:

   a) shall cache the information that the user homed in the IWF is in an in-progress emergency private call state with the targeted MCPTT user; and

   b) if this is a request for an MCPTT emergency alert, shall cache the information that the user homed in the IWF has sent an MCPTT emergency alert to the targeted user;

3) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.2.1;

4) if an implicit floor request is required, shall indicate this as specified in clause 6.7 and may include an application/vnd.3gpp.mcptt-location-info+xml MIME body with a <Report> element included in the <location-info> root element;

5) 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 homed in the IWF;

NOTE 1: How the IWF determines the MCPTT ID of a user homed in the IWF is out of scope of the present document.

6) shall include in the SIP re-INVITE request an SDP containing the current media parameters used by the existing session;

7) if this is a request for an MCPTT emergency alert:

   a) shall determine the value of the user's Mission Critical Organization identity; and.

NOTE 2: How the IWF determines the user's Mission Critical Organization identity is out of scope of the present document;

   b) shall include in the <mcpttinfo> element containing the <mcptt-Params> element containing an <mc-org> element set to the value of the user's Mission Critical Organization identity;

8) shall include a Resource-Priority header field populated with the values for an MCPTT emergency private call as specified in clause 6.6.3.1.12; and

9) shall send the SIP re-INVITE request towards the core network according to 3GPP TS 24.229 [3].

Upon receiving SIP 200 (OK) response for the SIP re-INVITE request the IWF performing the controlling role:

1) shall cache the contact received in the Contact header field;

2) shall interact with the user plane as specified in 3GPP TS 29.380 [31]; and

3) shall perform the actions specified in 3GPP TS 24.379 [29], clause 6.2.8.3.4 with the IWF acting as the MCPTT client.

11.1.3.6 Sending a SIP re-INVITE for cancellation of emergency private call

This clause 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 IWF performing the controlling role.

The IWF performing the controlling role:

1) shall generate a SIP re-INVITE request as specified 3GPP TS 24.379 [29], clause 6.3.3.1.9, with the IWF acting as the controlling function;

2) 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 user;

3) if this is a request for an MCPTT emergency alert cancellation, shall clear the cache of the MCPTT ID of user homed in the IWF as having an outstanding MCPTT emergency alert;

4) shall include an application/vnd.3gpp.mcptt-info+xml MIME body populated as specified in clause 6.4.2.3;

5) if an implicit floor request is required, shall indicate this as specified in clause 6.7;

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 homed in the IWF;

NOTE: How the IWF determines the MCPTT ID of a user homed in the IWF is out of scope of the present document.

7) shall include in the SIP re-INVITE request an SDP containing the current media parameters used by the existing session;

8) shall include a Resource-Priority header field populated with the values for a normal MCPTT private call as specified in clause 6.6.3.1.12; and

9) shall send the SIP re-INVITE request towards the core network according to 3GPP TS 24.229 [3].

Upon receiving SIP 200 (OK) response for the SIP re-INVITE request the IWF performing the controlling role:

1) shall cache the contact received in the Contact header field;

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) shall interact with the user plane as specified in 3GPP TS 29.380 [31].

11.2 Private call without floor control

11.2.1 Participating role procedures

11.2.1.1 Originating procedures

To request a private call without floor control, the IWF performing the participating role shall follow the procedures as specified in clause 11.1.2.1.1 for an on-demand session but with an SDP offer not including media-level section for media-floor control entity.

11.2.1.2 Terminating procedures

Upon receipt of a "SIP INVITE request for terminating participating MCPTT function" for the private call with SDP offer not including media-level section for media-floor control entity, the IWF performing the participating role consider it as the request for the private call without floor control and shall follow the procedures as specified in clause 11.1.2.2.

11.2.2 Controlling role procedures

11.2.2.1 Originating procedures

The IWF performing the controlling role shall follow the procedures as specified in clause 11.1.3.1.

11.3 Ending the private call initiated by a client

11.3.1 IWF performing the participating role procedures

11.3.1.1 Terminating procedures

11.3.1.1.1 Receipt of SIP BYE request for private call on-demand

Upon receiving a SIP BYE request from the controlling MCPTT function, the IWF performing the participating role shall follow the procedures as specified in clause 6.6.2.2.2.1.

11.4 Ending the private call initiated by the MCPTT server

11.4.1 Client derived procedures

11.4.1.1 Receiving a SIP BYE request for private call session

Upon receiving a SIP BYE request for private call session, the IWF shall follow the procedures as specified in clause 6.3.

11.4.2 IWF participating role procedures

11.4.2.1 Terminating procedures

11.4.2.1.1 Receipt of SIP BYE request for private call on-demand

Upon receiving a SIP BYE request from the controlling MCPTT function, the IWF performing the participating role shall follow the procedures as specified in clause 6.6.2.2.2.1.

11.4.3 IWF controlling role procedures

When the MCPTT session for private call needs to be released as specified in clause 6.6.7.2 with the IWF acting as the controlling MCPTT function, the IWF performing the controlling role shall follow the procedures in clause 6.6.3.1.2.

12 Emergency alert

12.1 IWF performing the participating role procedures

12.1.1 IWF to send SIP MESSAGE request for emergency notification

When the IWF performing originating participating role needs to send a SIP MESSAGE request for emergency notification, the IWF:

1) void;

2) if the MCPTT ID for which the SIP MESSAGE is sent is not affiliated with the MCPTT group as determined by clause 9.2.1.2.8, shall perform the actions specified in clause 9.2.1.2.9 for implicit affiliation;

3) if the actions for implicit affiliation specified in step 2) above were performed but not successful, shall skip the rest of the steps.

4) shall determine the public service identity of the controlling MCPTT function associated with the group identity in the received request for emergency notification;

5) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [3] and IETF RFC 3428 [18];

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 MCPTT group;

7) shall include an application/vnd.3gpp.mcptt-info+xml MIME body as specified in 3GPP TS 24.379 [29], clause F.1 included in the outgoing SIP MESSAGE request based on information received from signalling received from the originating LMR user and its network entities;

8) shall set the <mcptt-calling-user-id> element of the <mcpttinfo> element containing the <mcptt-Params> element to the MCPTT ID of the user homed in the IWF;

9) if location information is available in the received request for emergency notification, include an application/vnd.3gpp.mcptt-location-info+xml MIME body as specified in 3GPP TS 24.379 [29], clause F.3 in the outgoing SIP MESSAGE request;

10) shall set the P-Asserted-Identity in the outgoing SIP MESSAGE request to the public service identity of the IWF; and

11) shall send the SIP MESSAGE request as specified to 3GPP TS 24.229 [3].

Upon receipt of a SIP 2xx response to the SIP MESSAGE request:

1) if the procedures of clause 9.2.1.2.9 for implicit affiliation were performed in the present clause, shall complete the implicit affiliation by performing the procedures of clause 9.2.1.2.10.

Upon receipt of a SIP 4xx, 5xx or 6xx response to the sent SIP MESSAGE request and if the implicit affiliation procedures of clause 9.2.1.2.9 were invoked in the present clause, the IWF shall perform the procedures of clause 9.2.1.2.11.

12.1.2 Receipt of a SIP MESSAGE request for emergency notification for terminating LMR user

In the procedures in this clause:

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 request for emergency notification for terminating participating MCPTT function", the IWF performing the participating role:

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 IWF performing the participating role may include a Retry-After header field to the SIP 500 (Server Internal Error) response as specified in IETF RFC 3261 [14] 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 IWF 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 determine the terminating target; and

3) if the terminating target is not served by the IWF the IWF shall reject the SIP MESSAGE request with a SIP 404 (Not Found) response.

NOTE 2: LMR specific signalling is outside the scope of this specification.

The IWF shall generate s SIP 2xx response and follow the procedures specified in 3GPP TS 24.229 [3].

12.1.3 Receipt of a SIP MESSAGE request indicating successful delivery of emergency notification

Upon receipt of an indication for successful delivery of an emergency notification, internal actions performed by the IWF performing the terminating participating role are out of scope of the present document.

12.2 IWF controlling role procedures

12.2.1 Handling of a SIP MESSAGE request for emergency notification

Upon receipt of a "SIP MESSAGE request for emergency notification for controlling MCPTT function", the IWF performing the controlling role:

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 [14]. 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 clause 12.2.2 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 clause 6.6.3.1.8.1 shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request as specified in 3GPP TS 24.229 [3] 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 3GPP TS 24.379 [29], clause F.1 of 3GPP TS 24.379 [29] 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 [3] 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 clause 6.6.3.1.8.1:

      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 3GPP TS 24.379 [29], clause 6.3.6, with the IWF acting as the MCPTT server:

         I) shall check if the MCPTT user is eligible to be implicitly affiliated with the MCPTT group as determined by clause 9.2.1.3.6;

         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 clause 4.4 and skip the rest of the steps below; or

         III) if the procedures of clause 9.2.1.3.6 determined the MCPTT user to be eligible to be implicitly affiliated to the MCPTT group shall, perform the implicit affiliation as specified in clause 9.2.1.3.7;

      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 3GPP TS 24.379 [29], clause 6.3.3.1.11, with the IWF acting as the controlling MCPTT function, with the clarifications of clause 6.6.3.1.7;

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 [3];

iii) shall generate a SIP 200 (OK) response to the received SIP MESSAGE request as specified in 3GPP TS 24.229 [3] 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 [3].

v) shall generate a SIP MESSAGE request as described in 3GPP TS 24.379 [29], clause 6.3.3.1.20, with the IWF acting as the controlling MCPTT function, 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 [3].

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 [3].

If the IWF performing the controlling role needs to generate a SIP MESSAGE request for emergency notification, the IWF performing the controlling role:

1) for each of the affiliated MCPTT group members:

a) shall generate an outgoing SIP MESSAGE request notification of the MCPTT user's emergency alert indication as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11 with the IWF acting as the controlling MCPTT function, with the clarifications of clause 6.6.3.1.7;

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; and

c) shall send the SIP MESSAGE request according to according to rules and procedures of 3GPP TS 24.229 [3];

12.2.2 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 IWF performing the controlling role:

1) if the received SIP MESSAGE request is an unauthorised request for an MCPTT emergency alert cancellation as specified in clause 6.6.3.1.8.1:

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 clause 6.6.3.1.8.4, shall reject the SIP MESSAGE request with a SIP 403 (Forbidden) response to the SIP MESSAGE request as specified in 3GPP TS 24.229 [3] 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 3GPP TS 24.379 [29] 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 [3] 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 3GPP TS 24.379 [29] clause 6.6.3.1.8.4 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 request to the other affiliated and joined members of the MCPTT group as specified in clause 6.6.3.1.3. The IWF performing the controlling role:

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 [3]; and

B) upon receiving a SIP 200 (OK) response to the SIP re-INVITE request shall interact with the media plane as specified in 3GPP TS 29.380 [31];

iv) for each of the affiliated but not joined members of the group:

A) generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's emergency call as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11 with the IWF acting as the controlling MCPTT function;

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 [3];

vi) shall send the SIP 200 (OK) response to the received SIP MESSAGE as specified in 3GPP TS 24.229 [3] and skip the rest of the steps;

vii) shall generate a SIP MESSAGE request as described in 3GPP TS 24.379 [29], clause 6.3.3.1.20 with the IWF acting as the controlling MCPTT function 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 rules and procedures of 3GPP TS 24.229 [3]; and

2) if the received SIP MESSAGE request is an authorised request for an MCPTT emergency alert cancellation as specified in clause 6.6.3.1.8.1:

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 clause 6.6.3.1.8.4, for each of the affiliated but not joined members of the group:

   i) shall generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's emergency alert as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11 with the IWF acting as the controlling MCPTT function;

   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, shall 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 [3];

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 clause 6.6.3.1.8.4 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 clause 6.6.3.1.3. 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 [3]; and

      B) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request shall interact with the media plane as specified in 3GPP TS 29.380 [31]; 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 3GPP TS 24.379 [29], clause 6.3.3.1.11 with the IWF acting as the controlling MCPTT function;

      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 [3];

f) shall send the SIP 200 (OK) response to the received SIP MESSAGE as specified in 3GPP TS 24.229 [3].

g) shall generate a SIP MESSAGE request as described in 3GPP TS 24.379 [29], clause 6.3.3.1.20 with the IWF acting as the controlling MCPTT function 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 clause 6.6.3.1.8.4, 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 clause 6.6.3.1.8.4, 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 the rules and procedures of 3GPP TS 24.229 [3].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the IWF performing the controlling role shall follow the procedures specified in 3GPP TS 24.229 [3].

If the IWF performing the controlling role needs to generate a SIP MESSAGE for emergency alert cancellation, the IWF performing the controlling role:

1) if the in-progress emergency state of the MCPTT group is set to a value of "false", for each of the affiliated but not joined MCPTT members of the group:

a) shall generate a SIP MESSAGE request notification of the cancellation of the MCPTT user's emergency alert as specified in 3GPP TS 24.379 [29], clause 6.3.3.1.11 with the IWF acting as the controlling MCPTT function;

b) shall include an <originated-by> element in the application/vnd.3gpp.mcptt-info+xml MIME body in the outgoing SIP MESSAGE request set to the MCPTT ID of the user homed in the IWF;

c) 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

d) shall send the SIP MESSAGE request as specified in 3GPP TS 24.229 [3];

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

a) shall set the in-progress emergency state of the group to a value of "false";

b) cache the information that the outstanding in-progress emergency state of the group has been cancelled;

c) shall generate SIP re-INVITE requests to the other affiliated and joined MCPTT members of the MCPTT group as specified in clause 6.6.3.1.3. The IWF performing the controlling function:

i) for each affiliated and joined MCPTT member shall send the SIP re-INVITE request towards the MCPTT client as specified in 3GPP TS 24.229 [3]; and

ii) Upon receiving a SIP 200 (OK) response to the SIP re-INVITE request shall interact with the media plane as specified in 3GPP TS 29.380 [31]; and

d) for each of the affiliated but not joined MCPTT 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 3GPP TS 24.379 [29], clause 6.3.3.1.11 with the IWF acting as the controlling MCPTT function;

ii) 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 MCPTT ID of the user home in the IWF;

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

iv) 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

3) shall send the SIP MESSAGE requests according to the rules and procedures of 3GPP TS 24.229 [3].

Upon receipt of SIP 2xx responses to the outgoing SIP MESSAGE requests, the IWF performing the controlling role shall follow the procedures specified in 3GPP TS 24.229 [3].

13 Location procedures

13.1 General

It is outside the scope of this specification how the IWF performing the participating role configures a participant homed in the IWF to provide location information or how the IWF performing the participating role explicitly request a participant homed in the IWF to provide location information.

13.2 IWF participating role location procedures

13.2.1 General

The IWF performing participating role provides procedures to send a location information report from a participant homed in the IWF.

13.2.2 Location reporting configuration

Procedures for configuration of location reporting of participants homed in the IWF are out of scope of the current document.

13.2.3 Location reporting request

Procedures for requesting participants homed in the IWF to report location information are out of scope of the current document.

13.2.4 Location information report

The IWF performing the participating role uses location information of users homed in the IWF as appropriate.

14 Handling of Interworking Security Data messages

14.1 IWF

14.1.1 IWF originates Interworking Security Data message

Upon deciding to send an Interworking Security Data message, the IWF:

1) shall generate a SIP MESSAGE request in accordance with 3GPP TS 24.229 [3] and IETF RFC 3428 [18];

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 [5];

3) the IWF 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 [5];

4) 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

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

6) shall set the Request-URI to the address of the terminating participating function associated with the MC service ID of the targeted MC service user;

7) shall include a P-Asserted-Identity header field set to the public service identity of the IWF;

8) shall include an application/vnd.3gpp.interworking-data MIME body with the Interworking Security Data message payload as defined in clause 14.2.1;

9) if a security context between the MCPTT client and the IWF needs to be established and the security context does not exist or if the existing security context has expired, procedures in clause 11.2.2 in 3GPP TS 33.180 [29] shall be followed; and

10) send the SIP MESSAGE request according to rules and procedures of 3GPP TS 24.229 [3].

14.1.2 IWF receives Interworking Security Data message

Upon receiving a "SIP MESSAGE request for Interworking Security Data message for participating function", the actions performed by the IWF are out of scope of the present document. The received message, described in clause 14.2, contains an opaque payload, the contents of which are out of scope of the present document.

14.2 Interworking Security Data message payload

14.2.1 Message definition

This clause specifies the payload to be used when sending an Interworking Security Data message between the IWF and MCPTT clients. The Interworking Security Data (InterSD) message is defined as a MONP message.

Message type: InterSD-MESSAGE

Direction: IWF to MCPTT client, MCPTT client to IWF

Table 14.2.1-1: Interworking Security Data message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	SDS signalling payload message identity	Message type 3GPP TS 24.282 [30]	M	V	1
	External network type	14.2.2	M	V	1
7D	URI of LMR key management functional entity	URI encoded as specified in IETF RFC 3986 [32]	O	TLV-E	3-x
78	Payload	3GPP TS 24.282 [30], clause 15.2.13 with Payload content type set to 'BINARY'	O	TLV-E	3-x

14.2.2 External network type

The purpose of the external network type information element is to identify the type of the network represented by the IWF.

The value part of the external network type information element is coded as shown in Table 14.2.2-1.

The external network type information element is a type 3 information element with a length of 1 octet.

Table 14.2.2-1: External network type

Bits 8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 1	P25
0 0 0 0 0 0 1 0	TETRA
All other values are reserved.	

Annex A (normative): XML Schema

A.1 General

The XML schema elements defined in the present clause extend those in 3GPP TS 24.379 [29] or other 3GPP technical specifications as noted.

A.2 mcpttinfo

A.2.1 XML schema

The XML schema elements for private call parameters in the present clause extend the mcpttinfo schema in 3GPP TS 24.379 [29].

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:mgktp="urn:3gpp:ns:mcpttGKTP:1.0">

  <xs:element name="private-call-params" type="private-call-params-type"/>

  <xs:complexType name="private-call-params-type">
    <xs:sequence>
      <xs:choice minOccurs="0">
        <xs:element name="floor-control" type="emptyType"/>
        <xs:element name="without-floor-control" type="emptyType"/>
      </xs:choice>
      <xs:choice minOccurs="0">
        <xs:element name="implicit-floor" type="emptyType"/>
        <xs:element name="without-implicit-floor" type="emptyType"/>
      </xs:choice>
      <xs:choice minOccurs="0">
        <xs:element name="manual-commencement" type="emptyType"/>
        <xs:element name="automatic-commencement" type="emptyType"/>
      </xs:choice>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
  </xs:complexType>

  <!-- empty complex type -->
  <xs:complexType name="emptyType"/>

</xs:schema>
```

Editor's Note: Need to register and add a namespace to the schema that's specific to interworking.

A.2.2 Semantic

The <private-call-params> element may be included in the <anyExt> element of the <mcpttinfo> element, when responding to a SIP INVITE for a private call, with the following elements:

1) an element indicating support for the type of floor control:

   a) if the client supports private calls with floor control and the offer is for floor control, shall include a <floor-control> element;

   b) if the client supports private calls without floor control and the offer is for no floor control, shall include a <without-floor-control> element;

2) an element indicating support for type of first talker:

   a) if the client supports not talking first and the offer is for the caller to talk first, shall include an <implicit-floor> element; or

   b) if the client supports talking first and the offer is for the receiver to talk first, shall include a <without-implicit-floor> element; and

3) an element indicating support for type of commencement mode:

   a) if the client supports private calls with automatic commencement mode and the offer is for automatic commencement mode, shall include a <automatic-commencement> element; or

   b) if the client supports private calls with manual commencement mode and the offer is for manual commencement mode, shall include a <manual-commencement> element.

NOTE: The <private-call-params> element is only included in responses only from the IWF, not from the MCPTT system.

The <anyExt> element can be included with the following element not declared in the XML schema:

- a <request-type> of type "xs:string": set to value of "Interworking Security Data message" when a requesting an Interworking Security Data message.

Annex B (normative): IANA registration forms

B.1 Media type for transporting interworking data content

Your Name:

<MCC name>

Your Email Address:

<MCC email address>

Media Type Name:

Application

Subtype name:

vnd.3gpp.interworking-data

Required parameters:

None

Optional parameters:

None

Encoding considerations:

binary.

Security considerations:

General 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.

Security mechanisms specific to this media type are dependent upon the business and trust relationship between the Interworking function operator, the mission critical services operator and the SIP carrier operator. Mission critical services operators may wish to encrypt and integrity protect the content transported by this media type indepedently of mechanisms provided by the transport layer. Such mechanisms have been specified by 3GPP SA3.

The information transported in this media type does not include active or executable content.

This media type may 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:

The content transported within this media type does not need to be interpreted by a server as specific decisions are made based on the signalling content (e.g. store disposition history). The final destination point of the content is the terminating UE. Each UE and server that handles the content transported using this media type shall understand the definition of the messages and protocol elements as defined in 3GPP TS 29.379. Any messages and protocol elements not defined by 3GPP TS 29.379 shall be ignored by the recipient UE or server.

Published specification:

3GPP TS 29.379 "Mission Critical Push To Talk (MCPTT) call control interworking with LMR systems; Protocol specification", available via http://www.3gpp.org/specs/numbering.htm.

Application Usage:

Applications supporting the mission critical interworking with LMR systems procedures as described in the published specification. This media type shall contain LMR specific content that is related to the payload that is delivered to a terminating user or an application of the terminating user.

Fragment identifier considerations:

None.

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 C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-04						Initial version	0.0.0
2019-05						Contains agreed P-CRs from CT1#117: C1-193606, C1-193609, C1-193085, C1-193093, C1-193611, C1-193612, C1-193613, C1-193614, C1-193615, C1-193616, C1-193674, C1-193675, C1-193676	0.1.0
2019-06	CT#84	CP-191150				Presentation to TSG CT for information	1.0.0
2019-06						Rapporteur's fixes to bad references and editorials.	1.0.1
2019-08						Contains agreed P-CRs from CT1#117: C1-194202, C1-194204, C1-194206, C1-194208, C1-194209, C1-194212, C1-194802, C1-194804, C1-195016.	1.1.0
2019-10						Contains agreed P-CRs from CT1#120: C1-196207, C1-196870	1.2.0
2019-11						Contains agreed P-CRs from CT1#121: C1-198208, C1-198238, C1-198662, C1-198663, C1-198845	1.3.0
2019-12	CT#86	CP-193150				Presentation to TSG CT for approval	2.0.0
2019-12	CT#86	CP-193298				A title corrected	2.0.1
2019-12	CT#86					Version 16.0.0 created after approval	16.0.0
2020-09	CT#89e	CP-202161	0004		F	Correct XML schema	16.1.0
2020-09	CT#89e	CP-202162	0007	1	F	Correct MIME Subtype name in Annex B.1	16.1.0
2020-10	CT#89e					Correction to table of contents	16.1.1
2020-12	CT#90e	CP-203195	0011		F	Inter-SD message payload format alignment across domains	16.2.0
2020-12	CT#90e	CP-203195	0013		F	Remove EN in Annex B.1	16.2.0
2021-09	CT#93e	CP-212121	0018	-	F	Remove EN on end-to-end security	16.3.0
2021-09	CT#93e	CP-212121	0019	-	F	Remove ENs	16.3.0

History

Document history		
V16.0.0	November 2020	Publication
V16.1.1	November 2020	Publication
V16.2.0	January 2021	Publication
V16.3.0	October 2021	Publication