ETSI TS 136 579-1 V14.3.0 (2019-07)

LTE;
Mission Critical (MC) services over LTE;
Part 1: Common test environment
(3GPP TS 36.579-1 version 14.3.0 Release 14)

Reference
RTS/TSGR-0536579-1ve30

Keywords
LTE

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to 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.

The present document is part 1 of a multi-part deliverable covering conformance test specification for Mission Critical Services over LTE consisting of:

3GPP TS 36.579-1: "Mission Critical (MC) services over LTE; Part 1: Common test environment" (the present document)

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

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

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

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

In the present release of the specification only Mission Critical Push To Talk (MCPTT) Services are considered. Future releases may include other Mission Critical Services.

1 Scope

The present document defines the common test environment required for testing Client and Server implementations for compliance to the Mission Critical Services over LTE protocol requirements defined by 3GPP.

It contains definitions of reference conditions and test signals, default messages and other parameters, generic procedures, and, common requirements for test equipment with the goal for facilitating testing in general and test procedures specification in particular. Various parts of its content are referred to from other parts of the Mission Critical Services over LTE protocol conformance testing specification e.g. TS 36.579-2 [2] and TS 36.579-3 [3].

The present document does not define the common test environment required for testing the implementation of the underlying LTE protocols, i.e. the LTE bearers used for transport of the Mission Critical Services signalling and media. This is defined in TS 36.508 [6] and referred to from the present document whenever needed.

In regard to default messages or other information elements contents, the present document refers to content defined in requirements specifications specified by 3GPP or other organisations.

In the present release of the specification only Mission Critical Push To Talk (MCPTT) Services are considered. Future releases may include other Mission Critical Services.

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 36.579-2: "Mission Critical (MC) services over LTE; Part 2: Mission Critical Push To Talk (MCPTT) User Equipment (UE) Protocol conformance specification".

[3] 3GPP TS 36.579-3: "Mission Critical (MC) services over LTE; Part 3: Mission Critical Push To Talk (MCPTT) Server Application test specification".

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

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

[6] 3GPP TS 36.508: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); Common Test Environments for User Equipment (UE) Conformance Testing".

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

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

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

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

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

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

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

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

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

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

[17] Void

[18] Void

[19] Void

[20] Void

[21] Void

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

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

[24] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing".

[25] IETF RFC 6043: "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)".

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

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

[28] Void

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

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

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

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

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

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

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

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

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

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

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

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

[41] Void

[42] Void

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

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

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

[46] Void

[47] Void.

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

[49] Void

[50] IETF RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[51] IETF RFC 7913 (June 2016): "P-Access-Network-Info ABNF Update".

[52] IETF RFC 7315 (July 2014): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP".

[53] IETF RFC 3329: "TBD".

[54] IETF RFC 5031 (January 2008): "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

[55] IETF RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56] IETF RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[57] IETF RFC 7134: "The Management Policy of the Resource Priority Header (RPH) Registry Changed to "IETF Review"".

[58] IETF RFC 5621 (September 2009): "Message Body Handling in the Session Initiation Protocol (SIP)".

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

[60] IETF RFC 5009 (September 2007): "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[61] IETF RFC 3842 (August 2004) "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)".

[62] IETF RFC 6442 (December 2011): "Location Conveyance for the Session Initiation Protocol".

[63] IETF RFC 6335: "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry".

[64] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".

[65] 3GPP TS 23.032: "Universal Geographical Area Description (GAD)".

[66] 3GPP TS 26.171: "Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; General description".

[67] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[68] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[69] 3GPP TS 23.003: "Numbering, addressing and identification".

[70] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[71] Void

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

[73] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[74] 3GPP TS 36.523-3: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification; Part 3: Abstract Test Suites (ATS)".

[75] 3GPP TS 36.523-2: "User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".

[76] IETF RFC 3550: "TBD".

[77] IETF RFC 6749: "TBD".

[78] 3GPP TS 24.334: "Proximity-services (ProSe) User Equipment (UE) to ProSe function protocol aspects; Stage 3".

[79] 3GPP TS 31.101: "UICC-terminal interface; Physical and logical characteristics.

[80] 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[81] IETF RFC 6809 (November 2012): "Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)".

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

[83] IETF RFC 4826 (May 2007): " Extensible Markup Language (XML) Formats for Representing Resource Lists".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

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

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

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

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

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

MBMS subchannel

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

Pre-selected MCPTT user profile

3.2 Symbols

Void.

3.3 Abbreviations

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

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

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

4 General

4.1 MCPTT Conformance testing test points overview

Figure 4.1.1 provides a general overview of all MCPTT players which may have a role in different conformance testing scenarios together with virtual test points representing the information flow which is intended for conformance testing. The figure is mainly for descriptive purposes and may not necessarily represent a real MCPTT deployment or implementation.

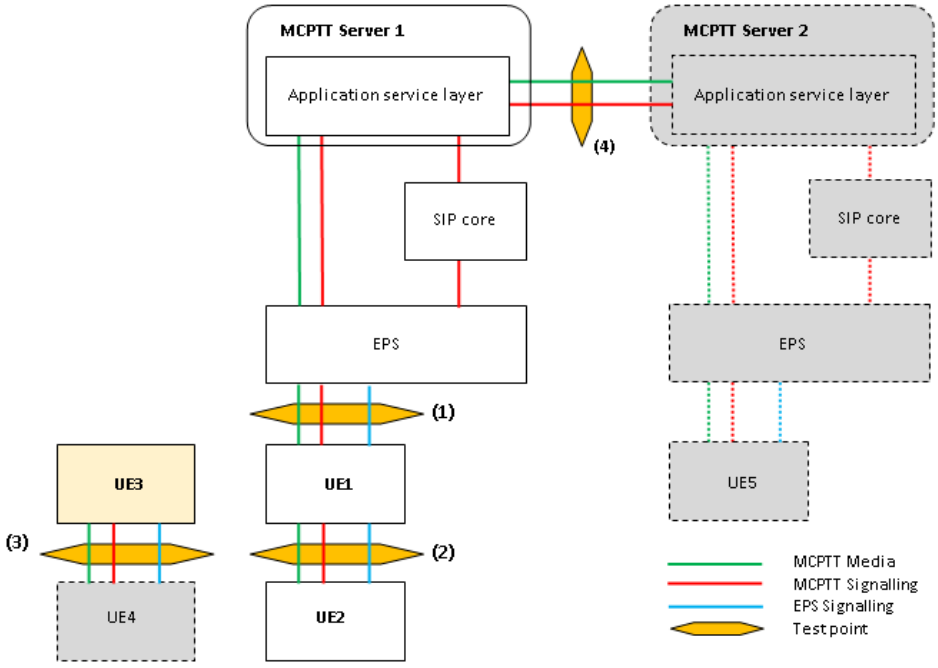

Figure 4.1.1: MCPTT Conformance testing test points model

NOTE 1: Which of the shown entities will be simulated and which will be real implementation depends on the test scenario. In the test scenarios in which they play a part, the entities presented with dashed borders and grey fill will be always simulated whereas, the entities with light yellow fill (UE3) will be Implementation Under Test (IUT). The entities with white fill will be either simulated or IUTs or real implementation (e.g. network) depending on the test scenario.

NOTE 2: While showing the different players, figure 4.1.1 should not be understood as showing test environment implementation.

The test points shown on Figure 4.1.1 cover behaviour/requirements observed at various reference points and communication scenarios:

- MCPTT on-network (whenever relevant, reference points as specified in TS 23.179 [8] Functional model description clause 7.3.1 'On-network functional model' are referred):
  - Application plane (MCPTT-1, MCPTT-4, MCPTT-7, MCPTT-8 and MCPTT-9), and, (CSC-1, CSC-2, CSC-4 and CSC-8); Signalling control plane (SIP-1, HTTP-1 and HTTP-2). Test point: (1) or (2). IUT: the UE or the MCPTT Server.
  - MCPTT-3 (between different MCPTT Servers), CSC-7 (other group management Servers, normally associated with other MCPTT Servers); Signalling control plane (SIP-2, HTTP-1, HTTP2 and HTTP-3). Test point: (4). IUT: the MCPTT Server.
- MCPTT off-network (TS 23.179 [8], clause 7.3.2 'Off-network functional model'). Test point: (3). IUT: the UE.
- LTE Legacy requirements between UE and EPS and between 2 UEs (covering e.g. Bearer Management at the UE side, ProSe including among others UE-to-network relay, MBMS). Test point: (1), (2) or (3).

Figure 4.1.2 provides a general overview of functions distributions at the MCPTT server side when multiple MCPTT Servers are involved. More functional models can be found in TS 24.379 [9].

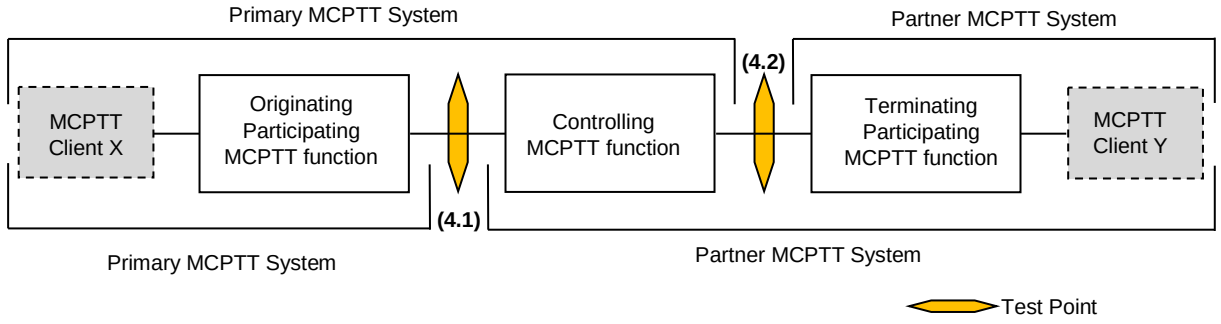

Figure 4.1.2: MCPTT Conformance testing Client-to-Client test points model

NOTE 3: While showing the different players and Server functionality, figure 4.1.2 should not be understood as showing test environment implementation.

The test points shown on Figure 4.1.2 provide an example of how 2 different communication scenarios between 2 MCPTT Servers will result in the communication between the servers being monitored at different test points (4.1) and (4.2). It should be noted that Figure 4.1.2 does not imply the physical existence of 2 test points during MCPTT Server-to-Server testing rather it shows two different information flows which need to be verified for conformance. In practice this will also mean that for testing the MCPTT Server on the Server-to-Server interface (test point 4 on Figure 4.1.1), the System Simulator (SS) will need to implement (i.e. be able to simulate) at least all 3 MCPTT functions.

4.2 MCPTT Conformance testing test environment overview

Based on the test points models shown in subclause 4.1 examples for test environment implementations are provided below. Figures 4.2.1 to 4.2.3 show test configuration where the Implementation Under Test (IUT) and the System

Simulator communicate, one with the other, over the LTE radio interface (test points (1), (2) and (3)). Figure 4.2.4 shows test configuration where the IUT and the system simulator, simulating MCPTT Clients, communicate, one with the other, over the LTE radio interface (test points (1)). Figures 4.2.5 and 4.2.6 show test configuration where the IUT and the System Simulator communicate, one with the other, over the MCPTT-3 interface, as defined by TS 23.179 [8], clause 7.5.2.4 (test points (4)).

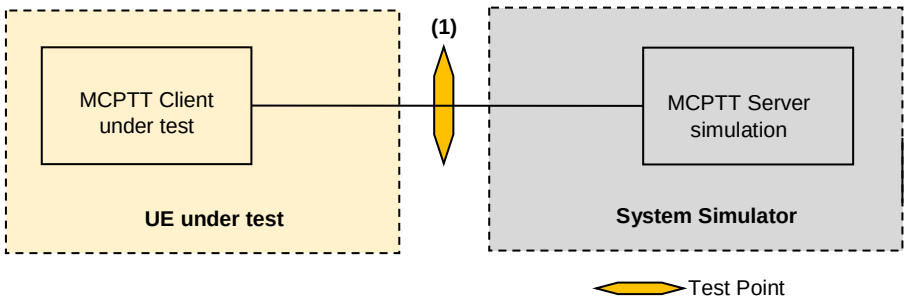

Figure 4.2.1: Testing the MCPTT Client (on-network)

NOTE 1: Figure 4.2.1 covers also the case for testing the UE at interface (1) when the IUT behaves as a Relay. For testing this the existence of another UE playing the role of an UE off-network which uses the Relay to connect to the Server will be needed. This could be implemented by the SS simulating both in similar manner as it is shown on Figure 4.2.2.

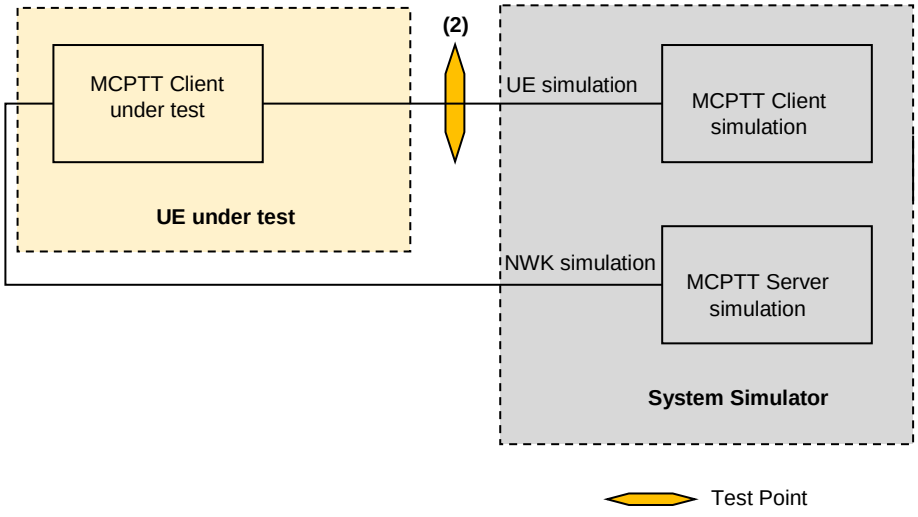

Figure 4.2.2: Testing the MCPTT Client (on-network) Relay side

NOTE 1: Figure 4.2.2 covers the case for testing the UE at interface (2) when the IUT behaves as a Relay. For testing this, the existence of LTE NWK and Server to which the Relay relays the data will be needed. This could be implemented by the SS simulating both.

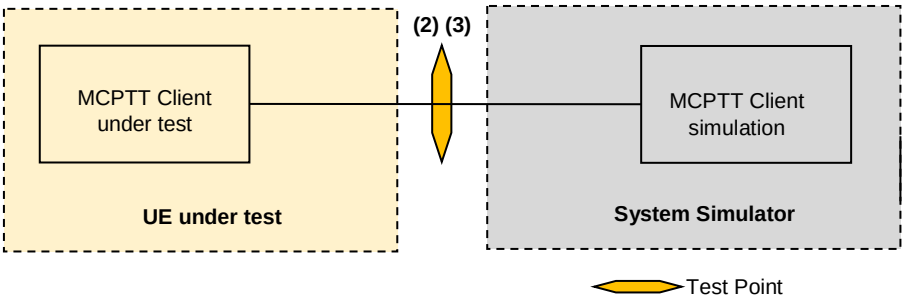

Figure 4.2.3: Testing the MCPTT Client (off-network)

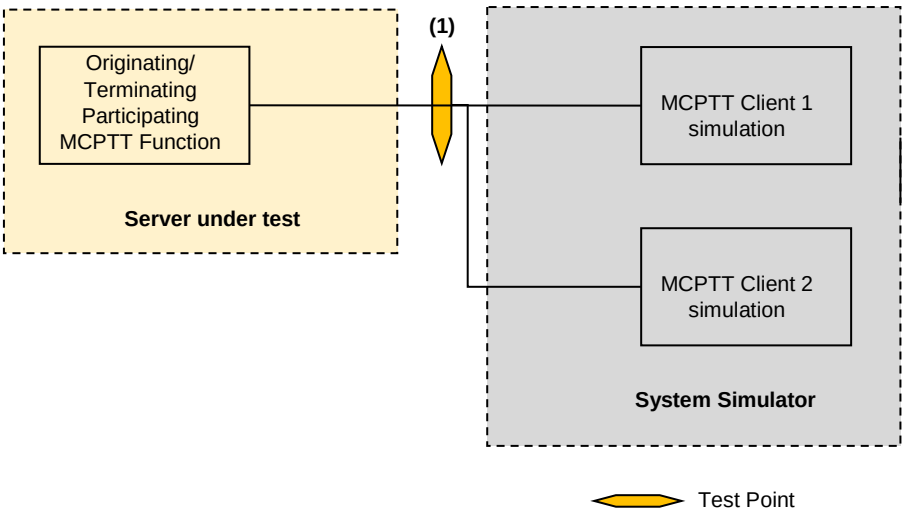

Figure 4.2.4: Testing the MCPTT Server (server-to-client)

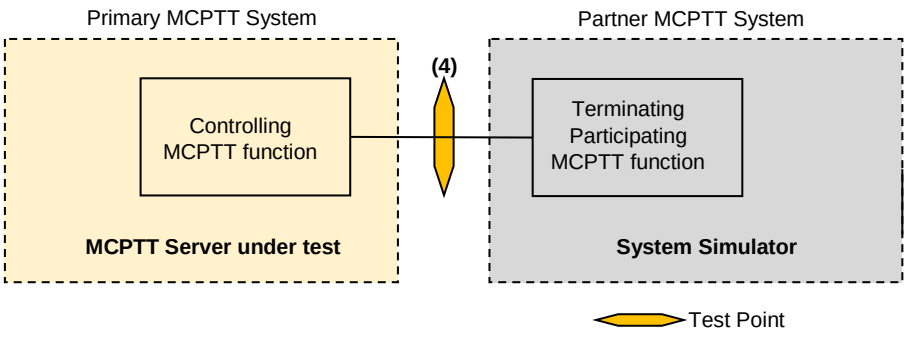

Figure 4.2.5: Testing the MCPTT Server (server-to-server), Controlling function

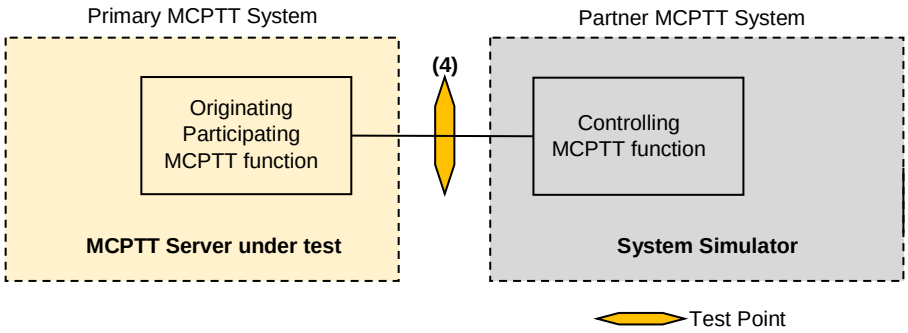

Figure 4.2.6: Testing the MCPTT Server (server-to-server), Originating function

4.3 MCPTT Conformance testing players and roles assumptions

Based on the described in clause 4.2 test environment scenarios a number of players and their roles have been designated to facilitate the test specification and provide a consistent test description.

For the purposes of MCPTT Client testing

1 MCPTT Server:

- Server A simulated by the SS (in the case of on-network operation).

2 MCPTT Clients:

- Client A installed on the implementation under test
- Client B simulated by the System Simulator (SS) either explicitly (in the case of off-network operations), or, implicitly (in the case of on-network operation).

3 MCPTT Users:

- User A registered with Client A and operating on the implementation under test
- User B registered with Client B simulated by the System Simulator (SS) either explicitly (in the case of off-network operations), or, implicitly (in the case of on-network operation); pre-set at User A configuration as User allowed to be called by User A for any types of calls
- User C known to the User A, not involved in any communication, defined for the sole purpose of testing if the User A/Client A can distinguish between different users when choosing one of them for action; pre-set at User A configuration as User allowed to be called by User A for any types of calls.

4 MCPTT groups:

- Group A to which User A is implicitly affiliated, pre-set at User A configuration, and, comprising as members User A, User B and User C, to be available throughout the entire testing.
- Group D to which User A is not implicitly affiliated, pre-set at User A configuration, and, comprising as members User B and User C, to be used for testing group affiliation.
- Groups B and C not pre-set at User A configuration, to be used for testing creation and termination of groups.

For the purposes of MCPTT Server testing

1 MCPTT Server:

- Server A installed on the implementation under test.

2 MCPTT Clients:

- Client A simulated by the System Simulator (SS)
- Client B simulated by the System Simulator (SS).

2 MCPTT Users:

- User A registered with Client A simulated by the System Simulator (SS) ; pre-set at User A configuration as User allowed to be called by User A for any types of calls
- User B registered with Client B simulated by the System Simulator (SS); pre-set at User A configuration as User allowed to be called by User A for any types of calls

1 MCPTT group:

- Group A to which User A is implicitly affiliated, pre-set at User A configuration, and, comprising as members User A and User B to be available throughout the entire testing.

5 Common Test Environment

5.1 General

Clause 5 provides basic test requirements, and, Generic Procedures and Default messages content to be used by the test cases wherever applicable.

5.2 Reference test conditions

5.2.1 General

Any E-UTRA frequency band can be used to provide the underlying communication bearer to carry the MCPTT communication. The requirements are defined in TS 36.508 [6].

5.2.2 On-network

There are no specific requirements to the UE on which the MCPTT client is installed when operating in on-network environment. The basic E-UTRA/EPC procedures shall be supported.

5.2.3 Off-network

When operating in off-network environment an MCPTT client shall:

- implement the procedures for ProSe direct discovery for public safety use as specified in 3GPP TS 24.334 [78];
- implement the procedures for one-to-one ProSe direct communication for Public Safety use as specified in 3GPP TS 24.334 [78].
- implement the procedures for one-to-many ProSe direct communication for Public Safety use as specified in 3GPP TS 24.334 [78].

5.3 Generic test procedures for UE MCPTT operation

5.3.1 General

The purpose of the procedures specified in the following subclauses is to facilitate test description by providing procedure sequences which can be referred from the relevant TCs specified e.g. in 3GPP TS 36.579-2 [2] or 3GPP TS 36.579-3 [3].

The procedures specified are required to ensure that any MCPTT service can take place or specific MCPTT relevant pre-conditions are met before a test case can be executed.

5.3.2 Generic Test Procedure for MCPTT Authorization/Configuration and Key Generation

5.3.2.1 Initial conditions

System Simulator:

- SS (MCPTT server)
  - For the underlying "transport bearer" over which the SS and the UE will communicate Parameters are set to the default parameters for the basic E-UTRA Single cell network scenarios, as defined in TS 36.508 [6] subclause 4.4. The simulated Cell 1 shall belong to PLMN1 (the PLMN specified for MCPTT operation in the MCPTT configuration document).

Implementation Under Test (IUT):

- UE (MCPTT client)
  - The MCPTT Client has been provisioned with the Initial UE Configuration Data as specified in subclause 5.5.8.1 allowing for the location of the configuration management server for configuration of the MCPTT UE initial configuration management object (MO) and the default MCPTT user profile configuration management object (MO).
  - UE and SS are configured to support one-way authentication based on server certificates (TS 33.179 [15] clause 5.4). For this purpose, self-signed certificates are pre-installed in the UE and SS.
  - The UE User is provided with username/password for user authentication (px_MCPTT_User_A_username, px_MCPTT_User_A_password as provided in TS 36.579-5 [5], Table 9.2-1: MCPTT Client Common PIXIT)
  - The test USIM set as defined in subclause 5.5.10 is inserted.

    The MCPTT client is attached to EPS services and then the UE is Switched OFF (state 1) according to TS 36.508 [6].

5.3.2.2 Definition of system information messages

The E-UTRA default system information messages as defined in TS 36.508 [6] are used.

5.3.2.3 Procedure

Table 5.3.2.3-1: MCPTT Authorization/Configuration and Key Generation

St	Procedure	Message Sequence	
		U - S	Message
1	Power up the UE.	-	-
-	EXCEPTION: The E-UTRA/EPC related actions which step 1 above will trigger are described in subclause 5.4.2 'Generic Test Procedure for MCPTT UE registration'. The test sequence below shows only the MCPTT relevant messages being exchanged.	-	-
2	Make the UE user request MCPTT service authorisation/configuration. NOTE 1 NOTE 1A	-	-
-	EXCEPTION: Steps 3a1-3b1 describe behaviour that depends on UE implementation of the OpenID Connect protocol; the "lower case letter" identifies a step sequence that take place when one or the other is the case.	-	-
3a1	The UE (MCPTT client) establishes a secure TLS tunnel as specified by 3GPP TS 33.310 [70], to the authorisation endpoint of the IdM server as specified in 3GPP TS 33.179 [15] using the configured URL of the authorisation endpoint of the IdM server as specified in the "<x>/OnNetwork/AppServerInfo/IDMSAuthEndpoint" leaf node, Table 5.5.8.1-1.	-	-
3a2	The UE (MCPTT client) sends an OpenID Connect Authentication Request using HTTP GET.	-->	HTTP GET (Authorization)
3b1	The UE (MCPTT client) sends an OpenID Connect Authentication Request using HTTP POST.	-->	HTTP POST (Authorization)
4	The SS sends a HTTP 200 (OK) including the HTML form requesting username and password.	<--	HTTP 200 (OK)
5	Make the UE user provide user credentials: username and password (px_MCPTT_User_A_username, px_MCPTT_User_A_password). NOTE 2	-	-
6	The UE (MCPTT client) sends an HTTP POST Request message to the SS containing user name and password.	-->	HTTP POST
7	The SS sends a HTTP 302 (Found) as the OpenID Connect Authentication Response containing an authorization code.	<--	HTTP 302 (Found)
-	EXCEPTION: Step 8a1 describes behaviour that depends on step 3 above. Step 8a1 only happens if the UE follows step 3b1, otherwise step 8a1 is skipped.	-	-
8a1	The UE (MCPTT client) establishes a secure TLS tunnel as specified by 3GPP TS 33.310 [70] to the token endpoint of the IdM server as specified in 3GPP TS 33.179 [15] using the configured URL of the token endpoint of the IdM server as specified in the "/<x>/OnNetwork/AppServerInfo/IDMSTokenEndpoint" leaf node, Table 5.5.8.1-1.	-	-
9	The UE (MCPTT client) sends an HTTP POST Request message to the SS over the TLS connection established to the IdM token endpoint (OIDC Token Request message), passing the authorization code obtained in step 7.	-->	HTTP POST
10	The SS sends a HTTP 200 (OK) providing id_token, access_token and refresh token.	<--	HTTP 200 (OK)
11	The UE (MCPTT client) sends a HTTP POST message presenting the access token obtained in step 10 to the SS over HTTP for Key Management Initialisation. NOTE: Step 11 is the start of the second stage which was started in Step 2. Steps 11 through 14 involve Key Management Authorization. The MCPTT Client/Key Management Client presents the access token to the Key Management Server. The end result is the user gets specific key material.	-->	HTTP POST

St	Procedure	Message Sequence	
		U - S	Message
12	The SS replies to the UE with identity specific key information.	<--	HTTP 200 (OK)
13	The UE (MCPTT client) sends a HTTP POST message presenting an access token to the SS over HTTP for Key Material Request.	-->	HTTP POST
14	The SS replies to the UE with identity specific key information.	<--	HTTP 200 (OK)
-	EXCEPTION: Steps 15a1-15b1 describe behaviour that depends on UE implementation ; the "lower case letter" identifies a step sequence that take place when one or the other is the case. NOTE: Step 15a1 is the start of the third stage which was started in Step 2. Steps 15a1, 15b1, and 16 involve User Service Authorization.	-	-
15a1	The UE (MCPTT client) sends a SIP REGISTER request for service authorisation.	-->	SIP REGISTER
15b1	The UE (MCPTT client) sends a SIP PUBLISH request for service authorisation.	-->	SIP PUBLISH
16	The SS (MCPTT server) sends SIP 200 (OK). NOTE: The user is now authorized for MCPTT service.	<--	SIP 200 (OK)
17	The UE (MCPTT client) sends a SIP SUBSCRIBE - subscription to multiple documents simultaneously - to the SS containing the access token and a resource list mime body containing a list of the following documents: MCPTT UE Configuration document, MCPTT User Profile Configuration Document, and the MCPTT Service configuration document. The base URI of each list entry is set to the CMS XCAP-ROOT-URI. NOTE: Step 17 is the start of the fourth stage which was started in Step 2. Steps 17 through 26 involve Configuration Management Authorization. The end result of the fourth stage is that the MCPTT Client receives 3 configuration documents: UE Configuration Document, User Profile Configuration Document, and the Service Configuration Document.	-->	SIP SUBSCRIBE
18	The SS sends a SIP 200 (OK) message.	<--	SIP 200 (OK)
19	The SS sends a SIP NOTIFY message to the UE that contains the XCAP-URI of the documents.	<--	SIP NOTIFY
20	The UE (MCPTT client) sends a SIP 200 (OK) message.	-->	SIP 200 (OK)
21	The UE (MCPTT client) sends an HTTP GET Request message to the SS that contains the access token and the XCAP-URI of the MCPTT UE Configuration Document. NOTE: The MCPTT Client is requesting the MCPTT UE Configuration Document.	-->	HTTP GET
22	The SS sends the HTTP 200 (OK) message including the MCPTT UE Configuration Document.	<--	HTTP 200 (OK)
23	The UE (MCPTT client) sends an HTTP GET Request message to the SS that contains the access token and the XCAP-URI of the MCPTT User Profile Configuration Document. NOTE: The MCPTT Client is requesting the MCPTT User Profile Configuration Document.	-->	HTTP GET
24	The SS sends the HTTP 200 (OK) message including the MCPTT User Profile Configuration Document. NOTE: The MCPTT User Profile Configuration Document includes information on MCPTT groups including for which groups the MCPTT Client is a member. The MCPTT User Profile Configuration Document includes Group A as a group for which the MCPTT Client is a member and is implicitly affiliated. Group A is used as the default group for all test cases in TS 36.579-2 and TS 36.579-3.	<--	HTTP 200 (OK)

St	Procedure	Message Sequence	
		U - S	Message
25	The UE (MCPTT client) sends an HTTP GET Request message to the SS that contains the access token and the XCAP-URI of the MCPTT Service Configuration Document. NOTE: The MCPTT Client is requesting the the MCPTT Service Configuration Document.	-->	HTTP GET
26	The SS sends the HTTP 200 (OK) message including the MCPTT Service Configuration Document.	<--	HTTP 200 (OK)
27	The UE (MCPTT client) sends a SIP SUBSCRIBE to the SS, containing the access token and a resource list mime body and a list of the Groups to be obtained. The base URI of each list entry is set to the GMS XCAP-ROOT-URI, and the MCPTT group ID identifies a group document. NOTE: Step 27 is the start of the fifth stage which was started in Step 2. Steps 27 through 32 involve Group Management Authorization. The end result is the MCPTT Client will receive group information for Group A. The MCPTT Client will also get the Group Master Key (GMK) for the group which will be used to derive keys for the group. There will also be a Group User Key Identifier (GUK-ID), and a Group Master Key Identifier (GMK-ID). According TS 33.179 [15], clause 7.36, the GMK shall be used as the MIKEY Traffic Generating Key (TGK) and the GUK-ID shall be used as the MIKEY CSB ID. These shall be used to generate the SRTP Master Key and SRTP Master Salt as specified in IETF RFC 3830 [24].	-->	SIP SUBSCRIBE
28	The SS sends a SIP 200 (OK) message.	<--	SIP 200 (OK)
29	The SS sends a SIP NOTIFY message to the UE that contains the XCAP-URI of the Group documents.	<--	SIP NOTIFY
30	The UE (MCPTT client) sends a SIP 200 (OK) message.	-->	SIP 200 (OK)
31	The UE (MCPTT client) sends an HTTP GET Request message to the SS that contains the access token and the XCAP-URI of the Group Configuration document.	-->	HTTP GET
32	The SS sends the HTTP 200 (OK) message including the Group Document 'MCPTT UE Configuration document'. NOTE 3	<--	HTTP 200 (OK)
-	EXCEPTION: SS releases the E-UTRA connection.	-	-

NOTE 1: This is expected to be done via a suitable implementation dependent mechanism and may be manually or automatically initiated.
NOTE 1A: This will start a 5 stage process. The first stage involves MCPTT User Authentication and includes Steps 3a1 through 10. The end result of the first stage is the MCPTT Client receives 3 tokens: access token, ID token, and refresh token.
NOTE 2: The UE is expected to prompt the MCPTT user for their username and password, or it may be stored on the UE. The provision of the username/password is expected to be done via a suitable implementation dependent MMI.
NOTE 3: This completes MCPTT service enabling on the UE.
NOTE 4: This is expected to be done via a suitable implementation dependent mechanism and may be manually or automatically initiated.

5.3.2.4 Specific message contents

Table 5.3.2.4-1: HTTP GET (Step 3a2, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.2-1, condition AUTH

Table 5.3.2.4-2: HTTP POST (Step 3b1, Table 5.1.3.2-1)

Derivation Path: Table 5.5.3.1-1, condition AUTH

Table 5.3.2.4-3: HTTP 200 (OK) (Step 4, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.10-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Message-body	<!DOCTYPE html> <html> <body> <form action=""> Username: <input type="text" name="user"> Password: <input type="password" name="password"> </form> </body> </html>			

Table 5.3.2.4-4: HTTP POST (Step 6, Table 5.1.3.2-1)

Derivation Path: Table 5.5.3.1-1, condition USERAUTH

Table 5.3.2.4-5: HTTP 302 (Found) (Step 7, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.8-1, condition AUTH.

Table 5.3.2.4-6: HTTP POST (Step 9, Table 5.1.3.2-1)

Derivation Path: Table 5.5.3.1-1, condition TOKEN

Table 5.3.2.4-7: HTTP 200 (OK) (Step 10, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.10-1, condition TOKEN

Table 5.3.2.4-8: HTTP POST (Step 11, Table 5.1.3.2-1)

Derivation Path: Table 5.5.3.1-1, condition KMSINIT.

Table 5.3.2.4-9: HTTP 200 (OK) (Step 12, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.10-1, condition KMSINIT.

Table 5.3.2.4-10: HTTP POST (Step 13, Table 5.1.3.2-1)

Derivation Path: Table 5.5.3.1-1, condition KMSKEY.

Table 5.3.2.4-11: HTTP 200 (OK) (Step 14, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.10-1, condition KMSKEY.

Table 5.3.2.4-12: SIP REGISTER (Step 15a1, Table 5.1.3.2-1)

Derivation Path: Table 5.5.2.13-1, condition CONFIG

Table 5.3.2.4-13: SIP PUBLISH (Step 15b1, Table 5.1.3.2-1)

Derivation Path: Table 5.5.2.11-1, condition CONFIG

Table 5.3.2.4-14: SIP SUBSCRIBE (Step 17, Table 5.1.3.2-1)

Derivation Path: Table 5.5.2.14-1, condition CONFIG

Table 5.3.2.4-15: SIP NOTIFY (Step 19, Table 5.1.3.2-1)

Derivation Path: Table 5.5.2.8-1, condition CONFIG

Table 5.3.2.4-16: HTTP GET (Step 21, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.2-1, condition UECONFIG.

Table 5.3.2.4-17: HTTP GET (Step 23, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.2-1, condition UEUSERPROF.

Table 5.3.2.4-18: HTTP GET (Step 25, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.2-1, condition UESERVCONFIG.

Table 5.3.2.4-19: HTTP 200 (OK) (Step 22, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.10-1, condition UECONFIG.

Table 5.3.2.4-20: HTTP 200 (OK) (Step 24, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.10-1, condition UEUSERPROF.

Table 5.3.2.4-21: HTTP 200 (OK) (Step 26, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.10-1, condition UESERVCONFIG.

Table 5.3.2.4-22: SIP SUBSCRIBE (Step 27, Table 5.1.3.2-1)

Derivation Path: Table 5.5.2.14-1, condition GROUPCONFIG				
Content-Type				
Content-Length				
Message-body				
MIME-Content-Type	"application/vnd.3gpp.mcptt-info+xml"			
MCPTT-Info	As described in Table 5.2.2.4-22A			

Table 5.3.2.4-22A: MCPTT-INFO in SIP SUBSCRIBE (Table 5.3.2.4-22)

Derivation Path: Table 5.5.2.22.2.2-1 condition CONFIG

Table 5.3.2.4-22B: SIP NOTIFY (Step 29, Table 5.1.3.2-1)

Derivation Path: Table 5.5.2.8-1, condition GROUPCONFIG

Table 5.3.2.4-23: HTTP GET (Step 31, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.2-1, condition GROUPCONFIG

Table 5.3.2.4-24: HTTP 200 (OK) (Step 32, Table 5.1.3.2-1)

Derivation Path: Table 5.5.4.10-1, condition GROUPCONFIG.

Table 5.3.2.4-25: Void

Table 5.3.2.4-26: SIP 200 (OK) (Step 16, 18, 28, Table 5.1.3.2-1))

Derivation Path: Table 5.5.2.17.1.2-1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Content-Type	Not included			

5.3.3 Generic Test Procedure for MCPTT pre-established session establishment CO

5.3.3.1 Initial conditions

System Simulator:

- SS (MCPTT server)
- For the underlying "transport bearer" over which the SS and the UE will communicate Parameters are set to the default parameters for the basic E-UTRA Single cell network scenarios, as defined in TS 36.508 [6] subclause 4.4. The simulated Cell 1 shall belong to PLMN1 (the PLMN specified for MCPTT operation in the MCPTT configuration document)

IUT:

- UE (MCPTT client)
  - The UE has performed the Generic Test Procedure for MCPTT Authorization/Configuration and Key Generation as specified in subclause 5.3.2 and thereby the MCPTT client is authorised for and able to use the MCPTT service including making group and private calls on- and off-network, and, the MCPTT user is registered for receiving MCPTT service through the MCPTT Client.

5.3.3.2 Definition of system information messages

The E-UTRA default system information messages as defined in TS 36.508 [6] are used.

5.3.3.3 Procedure

Table 5.3.3.3-1: MCPTT pre-established session establishment CO

St	Procedure	Message Sequence	
		U - S	Message
1	Make the UE (MCPTT User) request the creation of a pre-established session	-	-
-	EXCEPTION: The E-UTRA/EPC actions which are related to the MCPTT call establishment are described in subclause 5.4.3 'Generic Test Procedure for MCPTT CO communication in E-UTRA'. The test sequence below shows only the MCPTT relevant messages exchanged.	-	-
2-7	Void.	-	-
8	UE (MCPTT Client) sends a SIP INVITE message in order to create a pre-established session.	-->	SIP INVITE
9	Void.	-	-
10	The SS (MCPTT server) responds with a SIP 200 (OK) message.	<--	SIP 200 (OK)
11	UE (MCPTT client) notifies the user that the pre-established session has been created. NOTE: This is expected to be done via a suitable implementation dependent MMI.	-	-
12	The SS transmits an *RRCConnectionRelease* message.	<--	RRC: *RRCConnectionRelease*

5.3.3.4 Specific message contents

The MCPTT relevant SIP message contents are specified in the present document subclause 5.5.2.

5.4 Generic test procedures for UE operation over EUTRA/EPS

5.4.1 General

The purpose of the procedures specified in the following subclauses is to facilitate test description by providing procedure sequences which can be referred from the relevant TCs specified e.g. in 3GPP TS 36.579-2 [2] or 3GPP TS 36.579-3 [3].

The intention is, wherever possible, that E-UTRA/EPS signalling and initial conditions should not be provided in the test descriptions rather should be referred to the procedure steps described in the generic procedures below, whereas, the MCPTT SIP signalling and initial conditions when relevant for the test purposes shall be explicitly provided in the tests description itself.

Throughout the generic test procedures E-UTRA/EPC behaviour is denoted as "SS" for the System Simulator simulating the NWK side of the communication, and, "UE" for the Implementation Under Test (IUT), whereas the MCPTT relevant behaviour is denoted as "SS (MCPTT server)" and "UE (MCPTT client)"/"UE (MCPTT user)" respectively. ProSe related SS behaviour when the SS simulates an UE device is denoted e.g. as "SS-UE1".

Throughout the generic test procedures E-UTRA/EPC behaviour is denoted as "SS" for the System Simulator simulating the NWK side of the communication, and, "UE" for the Implementation Under Test (IUT), whereas the MCPTT relevant behaviour is denoted as "SS (MCPTT server)" and "UE (MCPTT client)"/"UE (MCPTT user)" respectively. ProSe related SS behaviour when the SS simulates an UE device is denoted e.g. as "SS-UE1".

5.4.1A UE APN/PDN support assumptions

A MCPTT (or in general Mission Critical Services) capable UE, depending on implementation/deployment, may be provided with up to 3 MCPTT related APN: An APN utilised by the MCPTT service including the MCPTT service APN for the SIP-1 reference point, an MC common core services APN for the HTTP-1 reference point and a MC identity management service APN for the CSC-1 reference point (see TS 23.179 [8], subclause 5.9).

To limit the test specification complexity utilisation of single APN/PDN to be used for all 3 MCPTT services is assumed and only 2 QCIs are used for the bearers established in regard to the PDN:

1. MCPTT (QCI=69 for signalling bearer, QCI=65 for voice), APN=px_MCPTT_ALL_APN

NOTE 1: It should be noted that the core specs impose a requirement that the QCI value 8 or better shall be used for the EPS bearer that transports HTTP-1 reference point messaging. Using a single APN and having for the EPS bearer QCI=69 will satisfy this.

NOTE 2: The px_MCPTT_ALL_APN is defined in TS 36.579-5 [5], and should be provided by the Device vendor in the initial UE configuration as specified in Table 5.5.8.1-1.

In addition to the MCPTT relevant APN, a MCPTT (or in general Mission Critical Services) capable UE may support 2 additional different APNs for which different PDNs each with its specific QCI:

2. Internet

3. IMS (VOLTE QCI=5 for signalling bearer, QCI=1 for voice call)

This will result in the need the MCPTT tests to be able to handle a 3 APNs and different PDNs.

NOTE 3: It should be noted that, handling IMS and MCPTT with one APN is theoretically possible but may have undesirable implications e.g. VoLTE signalling could delay MCPTT signalling therefore the assumption is that such implementations will be undesirable and unlikely.

Consequently, for the IMS and MCPTT it should be assumed that the UE will do 2 different registrations, i.e. for each of them there will be a separate TCP connection.

It is difficult to mandate any order of the UE requesting any of these 3 PDNs. Therefore any order should be handled in the test with special attention to the EPS bearer QCI which needs to be guaranteed by the SS depending on the APN being requested. It is expected that Devices shall obey the TS 24.301 [19], 6.5.1.2 requirements in regard to provision of APN name in the PDN CONNECTIVITY REQUEST message (the syntax for provision of the APN name is defined in TS 24.008 [20]). In order to facilitate handling the case when the MCPTT APN maybe the default APN and therefore, depending on implementation, the APN name for the default APN is not provided, a dedicated ICS for indicating if this is the case is specified in TS 36.579-4 [4].

In regard to the MCPTT the following shall be also taken into account

- If the PDN connection established during the initial attach by the UE is to an APN other than the MCPTT service APN, then prior to user authentication, the UE shall establish another PDN connection to the MCPTT service APN. PDN connection establishment can also be caused by a SIP registration request for MCPTT. The QCI value of 69 shall be used for the EPS bearer that transports SIP-1 reference point messaging. It is used for SIP signalling.

- For the MCPTT service APN, the MCPTT UE does not activate EPS bearers for media streams.

- The network initiates the creation of a dedicated bearer to transport the voice media. The dedicated bearer for Conversational Voice utilises the standardised QCI value of 65. The network, utilising dynamic PCC, creates no more than one dedicated bearer for voice media (the UE is required to support at minimum one UM bearer which is used for MCPTT voice).

5.4.2 Generic Test Procedure for MCPTT UE registration

5.4.2.1 Initial conditions

System Simulator:

- SS (MCPTT server)

- E-UTRA related parameters are set to the default parameters for the basic single cell environment, as defined in TS 36.508 [6] subclause 4.4, unless otherwise specified in the test case. Requirements in regard to the PLMN which the simulated Cell(s) belongs to are specified in the test case using the present procedure.

IUT:

- UE (MCPTT client)
  - The UE is MCPTT capable. The MCPTT preconditions required for initiation of MCPTT service authorization for the MCPTT client and the MCPTT service are specified in the test cases.
  - The test USIM set as defined in subclause 5.5.10 is inserted.
  - The UE shall be switched off.

5.4.2.2 Definition of system information messages

The E-UTRA default system information messages as defined in TS 36.508 [6] are used.

5.4.2.3 Procedure

Table 5.4.2.3-1: EUTRA/EPS signalling for UE registration

St	Procedure	Message Sequence	
		U - S	Message
0	Switch the UE on.	-	-
1	Make the UE initiate MCPTT service authorization for the MCPTT client and the MCPTT service.	-	-
2	UE transmits an *RRCConnectionRequest* message.	-->	RRC: *RRCConnectionRequest*
3	SS transmits an *RRCConnectionSetup* message.	<--	RRC: *RRCConnectionSetup*
4	The UE transmits an *RRCConnectionSetupComplete* message to confirm the successful completion of the connection establishment and to initiate the Attach procedure by including the ATTACH REQUEST message. The PDN CONNECTIVITY REQUEST message is piggybacked in ATTACH REQUEST. (NOTE 1)	-->	RRC: *RRCConnectionSetupComplete* NAS: ATTACH REQUEST NAS: PDN CONNECTIVITY REQUEST
5	The SS transmits an AUTHENTICATION REQUEST message to initiate the EPS authentication and AKA procedure.	<--	RRC: *DLInformationTransfer* NAS: AUTHENTICATION REQUEST
6	The UE transmits an AUTHENTICATION RESPONSE message and establishes mutual authentication.	-->	RRC: *ULInformationTransfer* NAS: AUTHENTICATION RESPONSE
7	The SS transmits a NAS SECURITY MODE COMMAND message to activate NAS security.	<--	RRC: *DLInformationTransfer* NAS: SECURITY MODE COMMAND
8	The UE transmits a NAS SECURITY MODE COMPLETE message and establishes the initial security configuration.	-->	RRC: *ULInformationTransfer* NAS: SECURITY MODE COMPLETE
-	EXCEPTION: Steps 9a1 to 9a2 describe behaviour that depends on UE configuration; the "lower case letter" identifies a step sequence that take place if the UE has ESM information which needs to be transferred.	-	-
9a1	IF the UE sets the ESM information transfer flag in the last PDN CONNECTIVITY REQUEST message THEN the SS transmits an ESM INFORMATION REQUEST message to initiate exchange of protocol configuration options and/or APN.	<--	RRC: *DLInformationTransfer* NAS: ESM INFORMATION REQUEST
9a2	The UE transmits an ESM INFORMATION RESPONSE message to transfer protocol configuration options and/or APN.	-->	RRC: *ULInformationTransfer* NAS: ESM INFORMATION RESPONSE
10	The SS transmits a *SecurityModeCommand* message to activate AS security.	<--	RRC: *SecurityModeCommand*
11	The UE transmits a *SecurityModeComplete* message and establishes the initial security configuration.	-->	RRC: *SecurityModeComplete*
12	The SS transmits a *UECapabilityEnquiry* message to initiate the UE radio access capability transfer procedure.	<--	RRC: *UECapabilityEnquiry*
13	The UE transmits a *UECapabilityInformation* message to transfer UE radio access capability.	-->	RRC: *UECapabilityInformation*
14	The SS transmits an *RRCConnectionReconfiguration* message to establish the default bearer with condition SRB2-DRB(1, 0) according to TS 36.508 [6] subclause 4.8.2.2.1.1. This message includes the ATTACH ACCEPT message. The ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message is piggybacked in ATTACH ACCEPT. (NOTE 1)	<--	RRC: *RRCConnectionReconfiguration* NAS: ATTACH ACCEPT NAS: ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST
15	The UE transmits an *RRCConnectionReconfigurationComplete* message to confirm the establishment of default bearer.	-->	RRC: RRCConnectionReconfigurationComplete
-	EXCEPTION: In parallel to the event described in step 16 below, if initiated by the UE the generic procedure for IP address allocation in the U-plane as defined in TS 36.508 [6] subclause 4.5A.1 takes place.	-	-
-	EXCEPTION: In parallel to the event described in step 16 below the events described in table 5.4.2.3-2 take place.	-	-
16	This message includes the ATTACH COMPLETE message. The ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message is piggybacked in ATTACH COMPLETE.	-->	RRC: ULInformationTransfer NAS: ATTACH COMPLETE NAS: ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT

St	Procedure	Message Sequence	
		U - S	Message
-	EXCEPTION: Depending on the UE capability step 16A may be performed 0, 1 or 2 times. (NOTE 1)	-	-
16A	The generic procedure for UE establishing additional PDN connectivity as specified in TS 36.508 [6] subclause 4.5A.16 takes place.	-	-
17	The SS transmits an *RRCConnectionRelease* message.	<--	RRC: *RRCConnectionRelease*
NOTE 1: The assumptions for the PDN support of a MCPTT capable UE, including the default EPS bearer context QCI requirements in regard to the different PDN are described in 5.4.1A.			

Table 5.4.2.3-2: SIP signalling for MCPTT UE registration

St	Procedure	Message Sequence	
		U - S	Message
1	The UE sends initial registration for IMS services.	-->	SIP REGISTER
2	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.	<--	SIP 401 Unauthorized
3	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.	-->	SIP REGISTER
4	The SS responds with 200 OK.	<--	SIP 200 OK
-	EXCEPTION: Steps 1a1 to 1b1 describe behaviour that depends on UE implementation and on availability of an access-token received as outcome of the user authentication procedure as described in 3GPP TS 24.482 [12]; the "lower case letter" identifies a step sequence that take place when one or the other is the case.	-	-
5a1	The UE (MCPTT client) sends a SIP REGISTER request for service authorisation.	-->	SIP REGISTER
5b1	The UE (MCPTT client) sends a SIP PUBLISH request for service authorisation.	-->	SIP PUBLISH
6	The SS (MCPTT server) sends SIP 200 (OK).	<--	SIP 200 (OK)
7	The SS (MCPTT server) sends SIP MESSAGE for configuring Location Info reporting.	<--	SIP MESSAGE
8	The UE (MCPTT client) responds with SIP 200 (OK)	-->	SIP 200 (OK)

5.4.2.4 Specific message contents

All specific EUTRA/EPS signalling message contents shall be referred to TS 36.508 [6] subclause 4.6 and 4.7.

The MCPTT relevant SIP message contents, Table 5.4.2.3-2, are specified in the present document subclause 5.5.2, except for the following messages.

Table 5.4.2.4-1: SIP MESSAGE (step 7)

Derivation Path: Table 5.5.2.7.2-1 SIP MESSAGE from the SS				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Content-Type				
MIME-Content-Type	"application/vnd.3gpp.mcptt-location-info+xml"		TS 24.379 [9] clause F.3	
Location-info	As described in Table 5.5.3.4.2-1: Location-info (Configuration sent by the SS)			

5.4.3 Generic Test Procedure for MCPTT CO communication in E-UTRA

5.4.3.1 Initial conditions

System Simulator:

- SS (MCPTT server)
- SS E-UTRA related parameters are set to the default parameters for the basic single cell environment, as defined in TS 36.508 [6] subclause 4.4, unless otherwise specified in the test case. Requirements in regard to the PLMN which the simulated Cell(s) belongs to are specified in the test case using the present procedure.

IUT:

- UE (MCPTT client)
  - The test USIM set as defined in subclause 5.5.10 is inserted.
  - The UE has performed the Generic Test Procedure for MCPTT UE registration as specified in subclause 5.4.2 and is in E-UTRA Registered, Idle Mode state with the MCPTT Client being active. During the attach a default EPS bearer context #3 (QCI 69) according to table 6.6.1-1, TS 36.508 [6] is established for MCPTT and SIP signalling.

  NOTE 1: The assumptions for the PDN support of a MCPTT capable UE, including the default EPS bearer context QCI requirements in regard to the different PDN are described in 5.4.1A.

  - Detailed initial conditions for the UE (MCPTT client) shall be specified in the TC referring to the present procedure.

5.4.3.2 Definition of system information messages

The E-UTRA default system information messages as defined in TS 36.508 [6] are used.

5.4.3.3 Procedure

Table 5.4.3.3-1: EUTRA/EPS signalling for MCPTT CO communication

St	Procedure	Message Sequence	
		U - S	Message
1	Make the UE attempt an MCPTT call	-	-
2	The UE transmits an *RRCConnectionRequest* message with ' establishmentCause' set to ' mo-Data '.	-->	*RRCConnectionRequest*
3	SS transmit an *RRCConnectionSetup* message.	<--	RRC: *RRCConnectionSetup*
4	The UE transmits an *RRCConnectionSetupComplete* message to confirm the successful completion of the connection establishment and to initiate the session management procedure by including the SERVICE REQUEST message.	-->	RRC: *RRCConnectionSetupComplete* NAS: SERVICE REQUEST
5	The SS transmits a *SecurityModeCommand* message to activate AS security.	<--	RRC: *SecurityModeCommand*
6	The UE transmits a *SecurityModeComplete* message and establishes the initial security configuration.	-->	RRC: *SecurityModeComplete*
7	The SS configures a new data radio bearer, associated with the default EPS bearer context. The *RRCConnectionReconfiguration* message is using condition SRB2-DRB(1, 0) as specified in TS 36.508 [6] subclause 4.8.2.2.1. The DRB associated with default EPS bearer context obtained during the attach procedure is established (see Preamble).	<--	RRC: *RRCConnectionReconfiguration*
-	EXCEPTION: In parallel to the events described in step 8 below, the events described in table 5.4.3.3-2 take place.	-	-

St	Procedure	Message Sequence	
		U - S	Message
8	The UE transmits an *RRCConnectionReconfigurationComplete* message to confirm the establishment of the new data radio bearer, associated with the default EPS bearer context.	-->	RRC: *RRCConnectionReconfigurationComplete*
9-12	Void.	-	-
13	The SS configures a new RLC-UM data radio bearer, associated with the dedicated EPS bearer context. *RRCConnectionReconfiguration* message contains the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message. EPS bearer context #5 (QCI 65) according to table 6.6.2-1: Reference dedicated EPS bearer contexts is used. NOTE 1: The same MCPTT PDN address is applicable because the linked EPS bearer ID refers to the default EBC.. NOTE 2: The network initiates the creation of a dedicated bearer to transport the voice media see 5.4.1A.	<--	RRC: *RRCConnectionReconfiguration* NAS: ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST
14	The UE transmits an *RRCConnectionReconfigurationComplete* message to confirm the establishment of the new data radio bearer, associated with the default EPS bearer for emergency IMS signalling.	-->	RRC: *RRCConnectionReconfigurationComplete*
15	The UE transmits an ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message.	-->	RRC: ULInformationTransfer NAS:ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT

Table 5.4.3.3-2: SIP signalling for MCPTT CO communication

St	Procedure	Message Sequence	
		U - S	Message
1	The UE (MCPTT client) sends an initial SIP INVITE request requesting the establishment of an MCPTT call.	-->	SIP INVITE
2	The SS (MCPTT server) sends SIP 183(Session Progress).	<--	SIP 183 (Session Progress)
3	The SS (MCPTT server) sends SIP 200 (OK).	<--	SIP 200 (OK)
NOTE: The SIP sequence described in the present table is based on MCPTT CO call establishment and is for descriptive purposes only. When a TC refers to the generic procedure described in the present subclause, the SIP sequence may be replaced as appropriate.			

5.4.3.4 Specific message contents

All specific EUTRA/EPS signalling message contents shall be referred to TS 36.508 [6] subclauses 4.6 and 4.7.

All specific SIP signalling message contents shall be specified in the TC which refers to the present procedure.

5.4.4 Generic Test Procedure for MCPTT CT communication in E-UTRA

5.4.4.1 Initial conditions

System Simulator:

- SS (MCPTT server)
- E-UTRA related parameters are set to the default parameters for the basic single cell environment, as defined in TS 36.508 [6] subclause 4.4, unless otherwise specified in the test case. Requirements in regard to the PLMN which the simulated Cell(s) belongs to are specified in the test case using the present procedure.

IUT:

- UE (MCPTT client):

  - The test USIM set as defined in subclause 5.5.10 is inserted.

  - The UE has performed the Generic Test Procedure for MCPTT UE registration as specified in subclause 5.4.2 and is in E-UTRA Registered, Idle Mode state with the MCPTT Client being active. During the attach a default EPS bearer context #3 (QCI 69) according to table 6.6.1-1, TS 36.508 [6] is established for MCPTT and SIP signalling.

NOTE 1: The assumptions for the PDN support of a MCPTT capable UE, including the default EPS bearer context QCI requirements in regard to the different PDN are described in 5.4.1A.

  - Detailed initial conditions for the UE (MCPTT client) shall be specified in the TC referring to the present procedure.

5.4.4.2 Definition of system information messages

The E-UTRA default system information messages as defined in TS 36.508 [6] are used.

5.4.4.3 Procedure

Table 5.4.4.3-1: EUTRA/EPS signalling for MCPTT CT communication

St	Procedure	Message Sequence	
		U - S	Message
1	SS sends a *Paging* message to the UE on the appropriate paging block, and including the UE identity in one entry of the IE *pagingRecordLists*.	<--	RRC: *Paging* (PCCH)
2	The UE transmits an *RRCConnectionRequest* message with ' establishmentCause' set to 'mt-Access'.	-->	*RRCConnectionRequest*
3	SS transmit an *RRCConnectionSetup* message.	<--	RRC: *RRCConnectionSetup*
4	The UE transmits an *RRCConnectionSetupComplete* message to confirm the successful completion of the connection establishment and to initiate the session management procedure by including the SERVICE REQUEST message.	-->	RRC: *RRCConnectionSetupComplete* NAS: SERVICE REQUEST
5	The SS transmits a *SecurityModeCommand* message to activate AS security.	<--	RRC: *SecurityModeCommand*
6	The UE transmits a *SecurityModeComplete* message and establishes the initial security configuration.	-->	RRC: *SecurityModeComplete*
7	The SS configures a new data radio bearer, associated with the default EPS bearer context. The *RRCConnectionReconfiguration* message is using condition SRB2-DRB(1, 0) as specified in TS 36.508 [6] subclause 4.8.2.2.1. The DRB associated with default EPS bearer context obtained during the attach procedure is established (see Preamble).	<--	RRC: *RRCConnectionReconfiguration*
-	EXCEPTION: In parallel to the events described in steps 11-15 below, the event described in step 1, table 5.4.4.3-2 takes place.	-	-
8	The UE transmits an *RRCConnectionReconfigurationComplete* message to confirm the establishment of the new data radio bearer, associated with the default EPS bearer context.	-->	RRC: *RRCConnectionReconfigurationComplete*
9-12	Void.	-	-

St	Procedure	Message Sequence	
		U - S	Message
13	The SS configures a new RLC-UM data radio bearer, associated with the dedicated EPS bearer context. *RRCConnectionReconfiguration* message contains the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message. EPS bearer context #5 (QCI 65/69) according to table 6.6.2-1: Reference dedicated EPS bearer contexts is used. NOTE 1: The same MCPTT PDN address is applicable because the linked EPS bearer ID refers to the default EBC. NOTE 2: The network initiates the creation of a dedicated bearer to transport the voice media see 5.4.1A.	<--	RRC: *RRCConnectionReconfiguration* NAS: ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST
14	The UE transmits an *RRCConnectionReconfigurationComplete* message to confirm the establishment of the new data radio bearer, associated with the default EPS bearer for emergency IMS signalling.	-->	RRC: *RRCConnectionReconfigurationComplete*
15	The UE transmits an ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message.	-->	RRC: ULInformationTransfer NAS:ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT
16	The event described in step 2, table 5.4.4.3-2 takes place.	-	-

Table 5.4.4.3-2: SIP signalling for MCPTT CT communication

St	Procedure	Message Sequence	
		U - S	Message
1	The SS (MCPTT Server) sends an initial SIP INVITE request requesting the establishment of an MCPTT call.	<--	SIP INVITE
2	The UE (MCPTT client) sends SIP 200 (OK).	-->	SIP 200 (OK)
NOTE: The SIP sequence described in the present table is based on MCPTT CO call establishment and is for descriptive purposes only. When a TC refers to the generic procedure described in the present subclause, the SIP sequence may be replaced as appropriate.			

5.4.4.4 Specific message contents

All specific EUTRA/EPS signalling message contents shall be referred to TS 36.508 [6] subclause 4.6 and 4.7.

All specific SIP signalling message contents shall be specified in the TC which refers to the present procedure.

5.4.5 Generic Test Procedure for MCPTT CO communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment

5.4.5.1 Initial conditions

System Simulator:

- SS-UE1 (MCPTT Client).
  - For the underlying "transport bearer" over which the SS and the UE will communicate, the SS is behaving as SS-UE1 as defined in TS 36.508 [6], configured for and operating as ProSe Direct Communication transmitting and receiving device.
- GNSS simulator configured to simulate a location in the centre of Geographical area #1 and providing timing reference as defined in TS 36.508 [6] Table 4.11.2-2 scenario #1, for the assistance of E-UTRAN off-network testing.

NOTE: For operation in off-network environment, it needs to be ensured that after the UE is powered up it considers the Geographical area #1 as being one of the geographical areas set in the USIM for operation when UE is "not served by E-UTRAN".

IUT:

- UE (MCPTT client):
  - The test USIM set as defined in subclause 5.5.10 is inserted.
  - Detailed initial conditions for the UE (MCPTT client) shall be specified in the TC referring to the present procedure.

UE state:

- The UE is in state Switched OFF (state 1) according to TS 36.508 [6].

5.4.5.2 Definition of system information messages

N/a (out of E-UTRA coverage)

5.4.5.3 Procedure

Table 5.4.5.3-1: ProSe direct communication one-to-one out of E-UTRA coverage signalling for MCPTT CO communication-establishment

St	Procedure	Message Sequence	
		U - S	Message
1	Power up the UE.	-	-
2	Wait for 15 sec to allow the UE to establish that it is out of coverage and initiate scanning the frequency pre-set for ProSe communication for any activities.	-	-
3	Make the UE initiate one-to-one ProSe direct communication with the remote UE preconfigured (ProSe Layer-2 Group ID).	-	-
4	UE sends a DIRECT_COMMUNICATION_REQUEST message, IP Address Config IE set to "address allocation not supported".	-->	DIRECT_COMMUNICATION_REQUEST
5	SS-UE1 sends a DIRECT_SECURITY_MODE_COMMAND message.	<--	DIRECT_SECURITY_MODE_COMMAND
6	UE sends a DIRECT_SECURITY_MODE_COMPLETE message ciphered and integrity protected with the new security context.	-->	DIRECT_SECURITY_MODE_COMPLETE
7	SS-UE1 sends a DIRECT_COMMUNICATION_ACCEPT message.	<--	DIRECT_COMMUNICATION_ACCEPT
8	EXCEPTION: After the communication is established, an IP address configuration procedure is performed depending on what the UE has indicated in the IP Address Config IE (if it is not "address allocation not supported") in the DIRECT_COMMUNICATION_REQUEST message, and, the SS-UE1 itself indicating "address allocation not supported" in the DIRECT_COMMUNICATION_ACCEPT message.	-	-
-	EXCEPTION: Steps 9a1 to 9a2 describe behaviour that depends on UE implementation; the "lower case letter" identifies a step sequence that depends on the UE implementation of keepalive procedure.	-	-
9a1	UE sends a DIRECT_COMMUNICATION_KEEPALIVE message.	-->	DIRECT_COMMUNICATION_KEEPALIVE
9a2	SS-UE1 sends a DIRECT_COMMUNICATION_KEEPALIVE_ACK message.	<--	DIRECT_COMMUNICATION_KEEPALIVE_ACK

5.4.5.4 Specific message contents

Table 5.4.5.4-1: DIRECT_COMMUNICATION_ACCEPT (step 7 Table 5.4.5.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-6.			
Information Element	**Value/remark**	**Comment**	**Condition**
IP Address Config	'0011'B	address allocation not supported	
Link Local IPv6 Address	If the UE indicated 'address allocation not supported' in the IP Address Config IE in the DIRECT_COMMUNICATION_REQUEST message then a link-local IPv6 address formed locally	128-bit IPv6 address	

Table 5.4.5.4-2: DIRECT_SECURITY_MODE_COMMAND (step 5, Table 5.4.5.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-7.			
Information Element	**Value/remark**	**Comment**	**Condition**
UE Security Capabilities	Set to the UE Security Capabilities received in the DIRECT_COMMUNICATION_REQUEST message		
Chosen Algorithms	One of the non-null algorithms provided in UE Security Capabilities (i.e. different to EIA0 (null integrity protection algorithm)/EEA0 (null ciphering algorithm))		
MSB of K_D ID	The MSB of KD ID of the new KD		
K_D Freshness	Not included		
GPI	Not included		
User Info {			
Type of User Info	IMSI		
Odd/even indication	Reflecting the number of digits in the IMSI		
Identity digits	A value different to the IMSI of the UE		
}			

Table 5.4.5.4-3: DIRECT_SECURITY_MODE_COMPLETE (step 6, Table 5.4.5.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-8.			
Information Element	**Value/remark**	**Comment**	**Condition**
LSB of KD ID	Not included		

Table 5.4.5.4-4: DIRECT_COMMUNICATION_KEEPALIVE (step 9a1, Table 5.4.5.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-9.			
Information Element	**Value/remark**	**Comment**	**Condition**
Keepalive Counter	0		
Maximum Inactivity Period	Any allowed value		

5.4.6 Generic Test Procedure for MCPTT CT communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment

5.4.6.1 Initial conditions

System Simulator:

- SS-UE1 (MCPTT Client).
  - For the underlying "transport bearer" over which the SS and the UE will communicate, the SS is behaving as SS-UE1 as defined in TS 36.508 [6], configured for and operating as ProSe Direct Communication transmitting and receiving device.
- GNSS simulator configured to simulate a location in the centre of Geographical area #1 and providing timing reference as defined in TS 36.508 [6] Table 4.11.2-2 scenario #1,for the assistance of E-UTRAN off-network testing.

NOTE: For operation in off-network environment, it needs to be ensured that after the UE is powered up it considers the Geographical area #1 as being one of the geographical areas set in the USIM for operation when UE is "not served by E-UTRAN".

IUT:

- UE (MCPTT client)
  - The test USIM set as defined in subclause 5.5.10 is inserted.
  - Detailed initial conditions for the UE (MCPTT client) shall be specified in the TC referring to the present procedure.

UE state:

- The UE is in state Switched OFF (state 1) according to TS 36.508 [6].

5.4.6.2 Definition of system information messages

N/a (out of E-UTRA coverage).

5.4.6.3 Procedure

Table 5.4.6.3-1: ProSe direct communication one-to-one out of E-UTRA coverage signalling for MCPTT CT communication-establishment

St	Procedure	Message Sequence	
		U - S	Message
1	Power up the UE.	-	-
2	Wait for 15 sec to allow the UE to establish that it is out of coverage and initiate scanning the frequency pre-set for ProSe communication for any activities.	-	-
3	SS-UE1 sends a DIRECT_COMMUNICATION_REQUEST message, IP Address Config IE set to "address allocation not supported".	<--	DIRECT_COMMUNICATION_REQUEST
4	UE sends a DIRECT_SECURITY_MODE_COMMAND message unciphered but integrity protected with the new security context.	-->	DIRECT_SECURITY_MODE_COMMAND
5	SS-UE1 sends a DIRECT_SECURITY_MODE_COMPLETE message ciphered and integrity protected with the new security context.	<--	DIRECT_SECURITY_MODE_COMPLETE
6	UE sends a DIRECT_COMMUNICATION_ACCEPT message.	-->	DIRECT_COMMUNICATION_ACCEPT
7	EXCEPTION: After the communication is established, an IP address configuration procedure is performed depending on what the UE has indicated in the IP Address Config IE (if it is not "address allocation not supported") in the DIRECT_COMMUNICATION_REQUEST message, and, the SS-UE1 itself indicating "address allocation not supported" in the DIRECT_COMMUNICATION_ACCEPT message.	-	-
8	SS-UE1 sends a DIRECT_COMMUNICATION_KEEPALIVE message with a Keepalive Counter IE that contains the value of the keepalive counter for this link=0, and a Maximum Inactivity Period IE.	<--	DIRECT_COMMUNICATION_KEEPALIVE
9	UE sends a DIRECT_COMMUNICATION_KEEPALIVE_ACK message including the Keepalive Counter IE set to the same value as that received in the DIRECT_COMMUNICATION_KEEPALIVE message.	-->	DIRECT_COMMUNICATION_KEEPALIVE_ACK

5.4.6.4 Specific message contents

Table 5.4.6.4-1: DIRECT_COMMUNICATION_REQUEST (step 3, Table 5.4.6.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-5.			
Information Element	**Value/remark**	**Comment**	**Condition**
User Info {			
Type of User Info	IMSI		
Odd/even indication	Reflecting the number of digits in the IMSI		
Identity digits	A value different to the IMSI of the UE		
}			
IP Address Config	'0011'B	address allocation not supported	
Maximum Inactivity Period	'10 0000 0000'B	512 sec, randomly chosen to allow sufficient time for a TC which uses this procedure to be completed without need to repeat the keepalive procedure	
Nonce_1			
UE Security Capabilities	01111111 01111111	All but null algorithms supported	
MSB of $K_{D\text{-}sess}$ ID	the 8 most significant bits of the KD-sess ID		
K_D ID	Not present		
Signature	the ECCSI signature calculated with the User Info and Nonce_1 as specified in 3GPP TS 33.303 [67]		
Link Local IPv6 Address	a link-local IPv6 address formed locally		

Table 5.4.6.4-2: DIRECT_SECURITY_MODE_COMMAND (step 4 Table 5.4.6.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-7.			
Information Element	**Value/remark**	**Comment**	**Condition**
MSB of K_D ID	Any allowed value		
K_D Freshness	Not included		
GPI	Not included		
Signature	The ECCSI signature calculated with the User Info and Nonce_1 as specified in 3GPP TS 33.303 [67]		
Encrypted Payload	The SAKKE payload generated as specified in 3GPP TS 33.303 [67].		

Table 5.4.6.4-3: DIRECT_SECURITY_MODE_COMPLETE (step 5, Table 5.4.6.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-8.			
Information Element	**Value/remark**	**Comment**	**Condition**
LSB of KD ID	16 least significant bits of KD ID		

Table 5.4.6.4-4: DIRECT_COMMUNICATION_KEEPALIVE (step 8, Table 5.4.6.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-9.			
Information Element	**Value/remark**	**Comment**	**Condition**
Keepalive Counter	0		
Maximum Inactivity Period	'10 0000 0000'B	512 sec, randomly chosen to allow sufficient time for a TC which uses this procedure to be completed without need to repeat the keepalive procedure	

5.4.7 Generic Test Procedure for MCPTT communication over ProSe direct one-to-one communication out of E-UTRA coverage - release by the SS

5.4.7.1 Initial conditions

System Simulator:

- SS-UE1 (MCPTT Client).

  - Same as those defined in the 'Generic Test Procedure for MCPTT CO communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.5, or, the 'Generic Test Procedure for MCPTT CT communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.6.

IUT:

- UE (MCPTT client)

  ProSe related configuration

  - Same as those defined in the 'Generic Test Procedure for MCPTT CO communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.5, or, the 'Generic Test Procedure for MCPTT CT communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.6.

UE state

  - The UE has established ProSe direct communication one-to-one out of E-UTRA coverage using the 'Generic Test Procedure for MCPTT CO communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.5, or, the 'Generic Test Procedure for MCPTT CT communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.6.

5.4.7.2 Definition of system information messages

N/a (out of E-UTRA coverage).

5.4.7.3 Procedure

Table 5.4.7.3-1: ProSe direct communication one-to-one out of E-UTRA coverage signalling for MCPTT communication - release by the SS

St	Procedure	Message Sequence	
		U - S	Message
1	SS-UE1 sends a DIRECT_COMMUNICATION_RELEASE message with a Release Reason IE indicating 'Direct Communication to peer UE no longer needed'.	<--	DIRECT_COMMUNICATION_RELEASE
2	UE sends a DIRECT_COMMUNICATION_RELEASE_ACCEPT message.	-->	DIRECT_COMMUNICATION_RELEASE_ACCEPT

5.4.7.4 Specific message contents

Table 5.4.7.4-1: DIRECT_COMMUNICATION_RELEASE (step 1, Table 5.4.7.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-11.			
Information Element	**Value/remark**	**Comment**	**Condition**
Release Reason	'0001'B	Direct communication to the peer UE no longer needed	

5.4.8 Generic Test Procedure for MCPTT communication over ProSe direct one-to-one communication out of E-UTRA coverage - release by the UE

5.4.8.1 Initial conditions

System Simulator:

- SS-UE1 (MCPTT Client).
  - Same as those defined in the 'Generic Test Procedure for MCPTT CO communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.5, or, the 'Generic Test Procedure for MCPTT CT communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.6.

IUT:

- UE (MCPTT client)

  ProSe related configuration
  - Same as those defined in the 'Generic Test Procedure for MCPTT CO communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.5, or, the 'Generic Test Procedure for MCPTT CT communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.6.

UE state

- The UE has established ProSe direct communication one-to-one out of E-UTRA coverage using the 'Generic Test Procedure for MCPTT CO communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.5, or, the 'Generic Test Procedure for MCPTT CT communication over ProSe direct one-to-one communication out of E-UTRA coverage-establishment', as described in subclause 5.4.6.

5.4.8.2 Definition of system information messages

N/a (out of E-UTRA coverage).

5.4.8.3 Procedure

Table 5.4.8.3-1: ProSe direct communication one-to-one out of E-UTRA coverage signalling for MCPTT communication - release by the UE

St	Procedure	Message Sequence	
		U - S	Message
1	UE sends a DIRECT_COMMUNICATION_RELEASE message with a Release Reason IE indicating 'Direct Communication to peer UE no longer needed'.	-->	DIRECT_COMMUNICATION_RELEASE
2	SS-UE1 sends a DIRECT_COMMUNICATION_RELEASE_ACCEPT message.	<--	DIRECT_COMMUNICATION_RELEASE_ACCEPT

5.4.8.4 Specific message contents

Table 5.4.8.4-1: DIRECT_COMMUNICATION_RELEASE (step 1, Table 5.4.8.3-1)

Derivation path: 36.508 [6], Table 4.7F.3-11.			
Information Element	**Value/remark**	**Comment**	**Condition**
Release Reason	'0001'B	Direct communication to the peer UE no longer needed	

5.4.9 Generic Test Procedure for MCPTT communication in E-UTRA / Change of cells

5.4.9.1 Initial conditions

System Simulator:

- SS (MCPTT server)
- SS E-UTRA
  - Parameters are set to the default parameters for the basic E-UTRA single mode multi cell network scenarios, as defined in TS 36.508 [6] subclause 4.4, unless otherwise specified in the test case.
  - 3 cells (Cell 1, Cell 2 and Cell 4, all operating on the same frequency). Cells 1 and 2 are on the same PLMN1, whereas Cell 4 is on a different PLMN2.

NOTE: The procedure only requires at maximum 2 cells to be active at any one instance.

IUT:

- UE (MCPTT client)
  - The UE has performed the Generic Test Procedure for MCPTT UE registration as specified in subclause 5.4.2 and is in E-UTRA Registered, Idle Mode state on Cell 1 with the MCPTT Client being active. During the attach a default EPS bearer context #3 (QCI 69) according to table 6.6.1-1, TS 36.508 [6] is established for for MCPTT and SIP signalling. The UE is allowed to operate on both PLMN1 and PLMN2.

NOTE 1: The assumptions for the PDN support of a MCPTT capable UE, including the default EPS bearer context QCI requirements in regard to the different PDN are described in 5.4.1A.

- The UE has performed the Generic Test Procedure for MCPTT Authorization/Configuration and Key Generation as specified in subclause 5.3.2 and thereby the MCPTT client is authorised for and able to use the MCPTT service including making group and private calls on- and off-network, and, the MCPTT user is registered for receiving MCPTT service through the MCPTT Client. The PLMN1 is set as HPLMN and PLMN2 is set as VPLMN in Table 5.5.8.1-1: MCPTT Initial UE Configuration Defaults.

- Detailed initial conditions for the UE (MCPTT client) shall be specified in the TC referring to the present procedure.

5.4.9.2 Definition of system information messages

The E-UTRA default system information messages as defined in TS 36.508 [6] are used.

5.4.9.3 Procedure

Table 5.4.9.3-1 illustrates the downlink power levels and other changing parameters to be applied for the cells at various time instants of the test execution. Row marked "T0" denotes the initial conditions after preamble, while columns marked "T1" ... "Tn" are to be applied subsequently. The exact instants on which these values shall be applied are described elsewhere in the present clause.

Table 5.4.9.3-1: Time instances of cell power level and parameter changes

	Parameter	Unit	Cell 1	Cell 2	Cell 4
T0	Cell-specific RS EPRE	dBm/15k Hz	-79	"Off"	"Off"
T1	Cell-specific RS EPRE	dBm/15k Hz	"Off"	-79	"Off"
T2	Cell-specific RS EPRE	dBm/15k Hz	"Off"	"Off"	-79

Table 5.4.9.3-2: EUTRA/EPS signalling for UE changing cells

St	Procedure	Message Sequence	
		U - S	Message
1	The SS configures: Cell 1 and Cell 2 parameters according to the row "T1" in table 5.4.9.3-1 in order to simulate needs for cell reselection to Cell2.	-	-
2	Wait for 5 sec to allow the UE to adjust to cell changes. NOTE 1.	-	-
3	The SS configures: Cell 2 and Cell 4 parameters according to the row "T2" in table 5.4.9.3-1 in order to simulate needs for cell reselection to Cell4.	-	-
4	The Generic test procedure for 'Tracking area updating procedure' defined in TS 36.508 [6] subclause 4.5A.2 take place. NOTE 2.	-	-
NOTE 1: Depending on implementation the UE may start transmitting MCPTT protocol relevant data earlier. What may be transmitted is specified in the TCs. NOTE 2: The UE may start transmitting MCPTT protocol relevant data as soon as it receives TRACKING AREA UPDATE ACCEPT message. If this happens the SS shall not execute step 7 of the Generic test procedure for 'Tracking area updating procedure' and shall continue with the rest of the messages exchange defined in the test case.			

5.4.9.4 Specific message contents

None.

5.4.10 Generic Test Procedure for MCPTT CT communication over ProSe direct one-to-many communication out of E-UTRA coverage / Announcing/Discoveree procedure for group member discovery

5.4.10.1 Initial conditions

System Simulator:

- SS-UE1 (MCPTT Client).
  - For the underlying "transport bearer" over which the SS and the UE will communicate, the SS is behaving as SS-UE1 as defined in TS 36.508 [6], configured for and operating as ProSe Direct Communication transmitting and receiving device.
- GNSS simulator configured to simulate a location in the centre of Geographical area #1 and providing timing reference as defined in TS 36.508 [6] Table 4.11.2-2 scenario #1, for the assistance of E-UTRAN off-network testing.

NOTE: For operation in off-network environment, it needs to be ensured that after the UE is powered up it considers the Geographical area #1 as being one of the geographical areas set in the USIM for operation when UE is "not served by E-UTRAN".

IUT:

- UE (MCPTT client)
  - The test USIM set as defined in subclause 5.5.10 is inserted.
  - Detailed initial conditions for the UE (MCPTT client) shall be specified in the TC referring to the present procedure.

UE state:

- The UE is in state Switched OFF (state 1) according to TS 36.508 [6].

5.4.10.2 Definition of system information messages

N/a (out of E-UTRA coverage)

5.4.10.3 Procedure

Table 5.4.10.3-1: ProSe Direct Discovery for public safety use / Announcing/Discoveree procedure for group member discovery for MCPTT off-network CT group calls

St	Procedure	Message Sequence	
		U - S	Message
1	Power up the UE.	-	-
2	Wait for 60 sec to allow the UE to determine that it is in the Geographical area #1 set in the USIM for operation when UE is "not served by E-UTRAN and acquire reference timing.	-	-
-	EXCEPTION: Steps 3a1-3b3b1 describe events which depend on the UE capabilities; the "lower case letter" identifies a step sequence that takes place if the UE is capable or not of Announcing for group member discovery.	-	-
3a1	IF pc_ProSeAnnForGroupMemberDiscovery (TS 36.523-2 [75]) THEN Force the UE upper layer application corresponding to ProSe Application ID px_ProSeAnnApplicationIdentity2 (TS 36.523-3 [74]) to initiate continuous announcing its availability in a discovery group. NOTE 1.	-	-
3a2	The UE transmits in the next transmission period a PC5_DISCOVERY message for Group Member Discovery Announcement applying DUIK, DUSK, and DUCK with the associated Encrypted Bitmask, along with the UTC-based counter to the PC5_DISCOVERY message.	-->	PC5_DISCOVERY
3b1	ELSE SS sets WaitForMessageCounter=1	-	-
-	EXCEPTION: Steps 3b2-3b3b1 are repeated until the event described in step 3b3a1 takes place OR WaitForMessageCounter=11.	-	-
3b2	SS-UE1 transmits in the next transmission period a PC5_DISCOVERY message for Group Member Discovery Solicitation applying DUIK, DUSK, and DUCK with the associated Encrypted Bitmask, along with the UTC-based counter to the PC5_DISCOVERY message. WaitForMessageCounter=WaitForMessageCounter+1	<--	PC5_DISCOVERY
-	EXCEPTION: Steps 3b3a1-3b3b1 describe events which depend on the UE behaviour; the "lower case letter" identifies a step sequence that take place if the UE transmit or not in the next transmission period a PC5_DISCOVERY message.	-	-
3b3a1	The UE transmits in the next transmission period a PC5_DISCOVERY message for Group Member Discovery Response applying DUIK, DUSK, and DUCK with the associated Encrypted Bitmask, along with the UTC-based counter to the PC5_DISCOVERY message and including the target Discovery Group ID of the discovery group to be discovered in step 3b2.	-->	PC5_DISCOVERY
3b3b1	The WaitForMessageCounter=11.	-	-
-	EXCEPTION: Steps 4 and 5 may be repeated multiple times depending on the MCPTT procedure taking place.	-	-
-	EXCEPTION: Step 4 is repeated until the MCPTT protocol data unit provided by the higher layers is transmitted in full. NOTE 2.	-	-
4	SS-UE1 sends sidelink communication over the PC5 interface in the next transmission period using the timing reference provided by the GNSS simulator (same to be used by the UE). NOTE 3.	<--	*STCH PDCP SDU packet*
-	EXCEPTION: Step 5 is repeated until the MCPTT protocol data unit provided by the higher layers is transmitted in full. NOTE 4.	-	-
5	The UE sends sidelink communication over the PC5 interface in the next transmission period using the timing reference provided by the GNSS simulator (same to be used by the SS-UE1). NOTE 3.	-->	*STCH PDCP SDU packet*

NOTE 1: UEs which are capable of Announcing for group member discovery may start announcement automatically.
NOTE 2: The SS-UE1 may need to send more than one MCPTT protocol data unit in sequence with no response expected between them from the UE.
NOTE 3: What MCPTT protocol data units are included in the sidelink communication is defined in the test case using the present generic procedure.
NOTE 4: The UE may need to send more than one MCPTT protocol data unit in sequence with no response expected between them from the SS-UE1.

5.4.10.4 Specific message contents

Table 5.4.10.4-1: PC5_DISCOVERY (step 3a2 Table 5.4.10.3-1)

Derivation path: 36.508 [6], Table 4.7F.1-5A.

Table 5.4.10.4-2: PC5_DISCOVERY (step 3b2 Table 5.4.10.3-1)

Derivation path: 36.508 [6], Table 4.7F.1-5B.

Table 5.4.10.4-3: PC5_DISCOVERY (step 3b3a1 Table 5.4.10.3-1)

Derivation path: 36.508 [6], Table 4.7F.1-5C.

5.4.11 Generic Test Procedure for MCPTT CO communication over ProSe direct one-to-many communication out of E-UTRA coverage / Monitoring/Discoverer procedure for group member discovery / One-to-many communication

5.4.11.1 Initial conditions

System Simulator:

- SS-UE1 (MCPTT Client).
  - For the underlying "transport bearer" over which the SS and the UE will communicate, the SS is behaving as SS-UE1 as defined in TS 36.508 [6], configured for and operating as ProSe Direct Communication transmitting and receiving device.
- GNSS simulator configured to simulate a location in the centre of Geographical area #1 and providing timing reference as defined in TS 36.508 [6] Table 4.11.2-2 scenario #1, for the assistance of E-UTRAN off-network testing.

NOTE: For operation in off-network environment, it needs to be ensured that after the UE is powered up it considers the Geographical area #1 as being one of the geographical areas set in the USIM for operation when UE is "not served by E-UTRAN".

IUT:

- UE (MCPTT client)
  - The test USIM set as defined in subclause 5.5.10 is inserted.
  - Detailed initial conditions for the UE (MCPTT client) shall be specified in the TC referring to the present procedure.

UE state:

- The UE is in state Switched OFF (state 1) according to TS 36.508 [6].

5.4.11.2 Definition of system information messages

N/a (out of E-UTRA coverage)

5.4.11.3 Procedure

Table 5.4.11.3-1: ProSe Direct Discovery for public safety use / Monitoring/Discoverer procedure for group member discovery for MCPTT off-network CO group calls

St	Procedure	Message Sequence	
		U - S	Message
1	Power up the UE.	-	-
2	Wait for 60 sec to allow the UE to determine that it is in the Geographical area #1 set in the USIM for operation when UE is "not served by E-UTRAN and acquire reference timing.	-	-
-	EXCEPTION: Steps 3a1-3b3 describe events which depend on the UE capabilities; the "lower case letter" identifies a step sequence that takes place if the UE is capable or not of Monitoring for group member discovery.	-	-
3a1	IF pc_ProSeMonForGtoupMemberDiscovery (TS 36.523-2 [75]) THEN the SS-UE1 starts continuously transmitting in the relevant transmission periods a PC5_DISCOVERY message for Group Member Discovery Announcement applying DUIK, DUSK, and DUCK with the associated Encrypted Bitmask, along with the UTC-based counter to the PC5_DISCOVERY message.	<--	PC5_DISCOVERY
3b1	ELSE Force the UE upper layer application corresponding to ProSe Application ID px_ProSeAnnApplicationIdentity2 (TS 36.523-3 [74]) to solicit proximity of other UEs in a discovery group. NOTE 1.	-	-
3b2	The UE transmits in the next transmission period a PC5_DISCOVERY message for Group Member Discovery Solicitation applying DUIK, DUSK, and DUCK with the associated Encrypted Bitmask, along with the UTC-based counter to the PC5_DISCOVERY message.	-->	PC5_DISCOVERY
3b3	SS-UE1 transmits a PC5_DISCOVERY message for Group Member Discovery Response applying DUIK, DUSK, and DUCK with the associated Encrypted Bitmask, along with the UTC-based counter to the PC5_DISCOVERY message and including the target Discovery Group ID of the discovery group to be discovered in step 2b2.	<--	PC5_DISCOVERY
-	EXCEPTION: Steps 4 and 5 may be repeated multiple times depending on the MCPTT procedure taking place.	-	-
-	EXCEPTION: Step 4 is repeated until the MCPTT protocol data unit provided by the higher layers is transmitted in full. NOTE 2.	-	-
4	The UE sends sidelink communication over the PC5 interface in the next transmission period using the timing reference provided by the GNSS simulator (same to be used by the SS-UE1). NOTE 3.	-->	*STCH PDCP SDU packet*
-	EXCEPTION: Step 5 is repeated until the MCPTT protocol data unit provided by the higher layers is transmitted in full. NOTE 4.	-	-
5	SS-UE1 sends sidelink communication over the PC5 interface in the next transmission period using the timing reference provided by the GNSS simulator (same to be used by the UE). NOTE 3.	<--	*STCH PDCP SDU packet*

St	Procedure	Message Sequence	
		U - S	Message
NOTE 1: UEs which are not capable of Monitoring for group member discovery may start Discoverer procedure automatically. NOTE 2: The UE may need to send more than one MCPTT protocol data unit in sequence with no response expected between them from the SS-UE1. NOTE 3: Which MCPTT protocol data units are included in the sidelink communication is defined in the test case using the present generic procedure. NOTE 4: The SS-UE1 may need to send more than one MCPTT protocol data unit in sequence with no response expected between them from the UE.			

5.4.11.4 Specific message contents

Table 5.4.11.4-1: PC5_DISCOVERY (step 3a1 Table 5.4.11.3-1)

Derivation path: 36.508 [6], Table 4.7F.1-5A.

Table 5.4.11.4-2: PC5_DISCOVERY (step 3b2 Table 5.4.11.3-1)

Derivation path: 36.508 [6], Table 4.7F.1-5B.

Table 5.4.11.4-3: PC5_DISCOVERY (step 3b3 Table 5.4.11.3-1)

Derivation path: 36.508 [6], Table 4.7F.1-5C.

5.4.12 Generic Test Procedure for MCPTT communication over MBMS

5.4.12.1 Initial conditions

System Simulator:

- SS (MCPTT server)
- SS E-UTRA
  - E-UTRA related parameters are set to the default parameters for the basic single cell environment, as defined in TS 36.508 [6] subclause 4.4, unless otherwise specified in the test case.
  - MBSFNAreaConfiguration as defined in TS 36.508[6] table 4.6.1-4A is transmitted on MCCH

IUT:

- UE (MCPTT client):
  - E-UTRAN UE supporting MBMS services. The UE has performed the Generic Test Procedure for MCPTT UE registration as specified in subclause 5.4.2 and is in E-UTRA Registered, Idle Mode state. The UE is made interested in receiving MBMS service in the PLMN of Cell 1 with MBMS Service ID 0.
  - Detailed initial conditions for the UE (MCPTT client) shall be specified in the TC referring to the present procedure.

5.4.12.2 Definition of system information messages

The E-UTRA default system information messages as defined in TS 36.508 [6] are used. System information combination 15 as defined in TS 36.508[6] subclause 4.4.3.1 is used in the E-UTRA cell.

5.4.12.3 Procedure

Table 5.4.12.3-1: MCPTT communication over MBMS

St	Procedure	Message Sequence	
		U - S	Message
1	SS transmits *MBSFNAreaConfiguration* message	<--	*MBSFNAreaConfiguration*
2	Wait for a period equal to the MCCH modification period for the UE to receive *MBSFNAreaConfiguration* message.	-	-
-	EXCEPTION: Step 3 is repeated continuously to carry the relevant MCPTT protocol data units provided by the higher layers.	-	-
3	The SS transmits 1 MBMS Packet on the MTCH in the next MCH Scheduling Period. NOTE: Which MCPTT protocol data units are sent and at which time is defined in the test case using the present generic procedure.	<--	MBMS Packet

5.4.12.4 Specific message contents

None.

5.5 Default message and other information elements content

5.5.1 General

The following conditions apply throughout subclause 5.5:

Table 5.5.1-1: Conditions

Condition	Explanation
ON-NETWORK	Message/IE sent only in on-network scenario.
OFF-NETWORK	Message/IE sent only in off-network scenario.
PRIVATE-CALL	Message/IE sent only as part of a Private call handling.
GROUP-CALL	Message/IE sent only as part of a Group call handling.
EMERGENCY-CALL	Message/IE sent only as part of an Emergency call handling.
IMMPERIL-CALL	Message/IE sent only as part of an Immanent Peril call handling.
EMERGENCY-ALERT	Message/IE sent only as part of an Emergency Alert.
CONFIG	Message/IE sent only in configuration/authentication/authorisation scenario.
GROUPCONFIG	Message/IE sent only in group configuration scenario.

5.5.2 Default SIP message and other information elements

5.5.2.1 SIP ACK

5.5.2.1.1 SIP ACK from the UE

Table 5.5.2.1.1-1: SIP ACK from the UE

Derivation Path: TS 24.229 [16], subclause A.2.1.4.2, A.2.2.4.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22]	
Method	"ACK"			
Request-URI	px_MCPTT_Server_A_URI			
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value"	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with *'z9hG4bk'*		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	URIs of the Record-Route header sent to the UE in 183, 180 or 200 response (whichever response used for request message to be acknowledged and contained Record-Route header) in reverse order		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"	Local tag of the dialog ID		
To			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI			
tag	"2"	Remote tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	same value as in INVITE message			
Cseq			RFC 3261 [22]	
value	same value as in INVITE message			
method	"ACK"			
Max-Forwards			RFC 3261 [22]	
value	any allowed value	Non-zero value		
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.1.2 SIP ACK from the SS

Table 5.5.2.1.2-1: SIP ACK from the SS

Derivation Path: TS 24.229 [16], subclause A.2.1.4.2, A.2.2.4.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22]	
Method	"ACK"			
Request-URI	px_MCPTT_Client_B_ID			
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Client_B_ID":14000"			
via-branch	"z9hG4bkmcpttss2"	Value starting with *'z9hG4bk'*		
Route	not present		RFC 3261 [22]	
route-param	not present			
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI			
tag	"1"	Local tag of the dialog ID		
To			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"2"	Remote tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	px_MCPTT_CT_call_ID	Same value as in request message		
Cseq			RFC 3261 [22]	
value	"4711"	Same value as in request message		
method	"ACK"			
Max-Forwards			RFC 3261 [22]	
value	"70"	The recommended initial value is 70 in RFC 3261.		
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.2 SIP BYE

5.5.2.2.1 SIP BYE from the UE

Table 5.5.2.2.1-1: SIP BYE from the UE

Derivation Path: TS 24.229 [16], subclause A.2.1.4.3, A.2.2.4.3				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22]	
Method	"BYE"			
Request-URI	px_MCPTT_sesson_A_ID	The URI of the MCPTT session identity to leave		
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	same value as in INVITE message			
via-branch	any allowed value	Value starting with 'z9hG4bK'		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	URIs of the Record-Route header response in reverse order		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID	The URI of the UE		
tag	"1"	Local tag of the dialog ID		
To			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
tag	"2"	Remote tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	same value as in INVITE message			
CSeq			RFC 3261 [22]	
value	value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one			
method	"BYE"			
Require			RFC 3261 [22] RFC 3329 [50]	
option-tag	"sec-agree"			
Proxy-Require			RFC 3261 [22] RFC 3329 [50]	
option-tag	"sec-agree"			
Max-Forwards			RFC 3261[22]	
value	any allowed value	Non-zero value		
P-Access-Network-Info			RFC 7315 [52] RFC 7913 [51]	
access-net-spec	any allowed value	Access network technology and, if applicable, the cell ID		
P-Asserted-Identity			RFC 3325 [32]	
addr-spec	px_MCPTT_User_A_ID	The URI of the UE		
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.2.2 SIP BYE from the SS

Table 5.5.2.2.2-1: SIP BYE from the SS

Derivation Path: TS 24.229 [16], subclause A.2.1.4.3, A.2.2.4.3				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22]	
Method	"BYE"			
Request-URI	px_MCPTT_sesson_A_ID	The URI of the MCPTT session identity to leave		
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	same value as in INVITE message			
via-branch	"z9hG4bKmcpttss3"	Value starting with 'z9hG4bK'		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	URIs of the Record-Route header response in reverse order		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
tag	"1"	local tag of the dialog ID		
To			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID	The URI of the UE		
tag	"2"	remote tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	same value as in INVITE message			
CSeq			RFC 3261 [22]	
value	value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one			
method	"BYE"			
Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Proxy-Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Max-Forwards			RFC 3261[22]	
value	"70"	The recommended initial value is 70 in RFC 3261.		
P-Access-Network-Info	Not present		RFC 7315 [52] RFC 7913 [51]	
access-net-spec				
P-Asserted-Identity			RFC 3325 [32]	
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.3 SIP CANCEL

Table 5.5.2.3-1: SIP CANCEL

Derivation Path: TS 24.229 [16], subclause A.2.1.4.4, A.2.2.4.4				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22]	
Method	"CANCEL"			
Request-URI	same value as in the INVITE being cancelled			
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22]	
via-parm	same value as in the INVITE being cancelled			
From			RFC 3261 [22]	
addr-spec	same value as in the INVITE being cancelled			
tag	same value as in the INVITE being cancelled			
To			RFC 3261 [22]	
addr-spec	same value as in the INVITE being cancelled			
Call-ID			RFC 3261 [22]	
Callid	same value as in the INVITE being cancelled			
Session-ID			RFC 3261 [22]	
sess-id	same value as in the INVITE being cancelled			
CSeq			RFC 3261 [22]	
value	same value as in the INVITE being cancelled			
Method	"CANCEL"			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.4 SIP INFO

Table 5.5.2.4-1: SIP INFO

Derivation Path: TS 24.229 [16], subclause A.2.1.4.6, A.2.2.4.6				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Method	"INFO"			
Request-URI	px_MCPTT_Client_A_ID"			
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"			
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Server_A_URI			
Call-ID			RFC 3261 [22]	
Callid	same value as in the INVITE			
CSeq			RFC 3261 [22]	
value	value of CSeq sent by the SS within its previous request in the same dialog but increased by one			
Method	"INFO"			
Max-Forwards			RFC 3261 [22]	
value	any allowed value	Non-zero value		
Content-Length			RFC 3261 [22]	
value	length of message body			
Message Body	any allowed value			

5.5.2.5 SIP INVITE

5.5.2.5.1 SIP INVITE from the UE

Table 5.5.2.5.1-1: SIP INVITE from the UE

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7, A.2.2.4.7				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"INVITE"			
Request-URI	px_MCPTT_Server_A_URI	The public service identity identifying the participating MCPTT function serving the MCPTT user		
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with 'z9hG4bK'		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	<sip:SS P-CSCF address: protected server port of SS;lr>, <sip:px_scscf;lr>		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"			
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Server_A_URI			
Call-ID			RFC 3261 [22]	
callid	any allowed value			
CSeq			RFC 3261 [22]	
value	any allowed value			
method	"INVITE"			
Supported			RFC 3261 [22]	
option-tag	"timer"			
Session-Expires			RFC 4028 [30]	
generic-param	any allowed value			
P-Early-Media			RFC 5009 [60]	
em-parm	"inactive"			
Require			RFC 3261 [22] RFC 3312 [56] RFC 3329 [53]	
option-tag	"sec-agree"			
Proxy-Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Contact			RFC 3261 [22 RFC 3840 [33]	

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7, A.2.2.4.7				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
addr-spec	"sip:[5555::aaa:bbb:ccc :eee]"	SIP URI with IP address or FQDN and protected server port of UE		
	px_MCPTT_Client_A_I D":"protected server port as chosen by the UE			
feature-param	"+g.3gpp.mcptt"	This media feature tag when used in a SIP request or a SIP response indicates that the function sending the SIP message supports Mission Critical Push To Talk (MCPTT) communication.		
feature-param	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"	This URN indicates that the device has the capabilities to support the mission critical push to talk (MCPTT) service.		
feature-param	"audio"	This feature tag indicates that the device supports audio as a streaming media type.		
Max-Forwards			RFC 3261 [22]	
value	any allowed value	Non-zero value		
P-Access-Network-Info			RFC 7315 [52]	
access-net-specs	any allowed value	Access network technology and, if applicable, the cell ID		
Accept			RFC 3261 [22]	
media-range	"application/sdp, application/vnd.3gpp.mcptt-info+xml"			
P-Preferred-Service			RFC 6050 [31]	
Service-ID	"urn:urn-7:3gpp-service.ims.icsi.mcptt"			
P-Preferred-Identity			RFC 3325 [32]	
PPreferredID-value	px_MCPTT_User_A_ID	Contains the public user identity of the MCPTT user		
Accept-Contact			RFC 3841 [29]	
ac-value	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"			
req-param	"require"			
explicit-param	"explicit"			
Accept-Contact			RFC 3841 [29]	
ac-value	"+g.3gpp.mcptt"			
req-param	"require"			
explicit-param	"explicit"			
Answer-Mode			RFC 5373 [34]	
answer-mode-value	"Auto"			
Resource-Priority			RFC 4412 [40] RFC 7134 [57] RFC 8101 [45]	EMERGENCY-CALL or IMMPERIL-CALL

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7, A.2.2.4.7				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
r-value	"mcpttp.value"	"value" set to the value of the <resource-priority-namespace> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration documents		EMERGENCY-CALL
r-value	"mcpttq.value"	"value" set to the value of the <resource-priority-priority> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document		EMERGENCY-CALL
r-value	"mcpttp.value"	"value" set to the value of the <resource-priority-namespace> element contained in the <imminent-peril-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration documents		IMMPERIL-CALL
r-value	"mcpttq.value"	"value" set to the value of the <resource-priority-priority> element contained in the <imminent-peril-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document		IMMPERIL-CALL
Content-Type	"multipart/mixed"		RFC 5621 [58]	
Content-Length	length of message body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/sdp"		RFC 4566 [27]	
SDP Message	As described in Table 5.5.3.1.1-1			
MIME-Content-Type	"application/vnd.3gpp.mcptt-info+xml"		TS 24.379 [9] clause F.1	
MCPTT-Info	As described in Table 5.5.3.2.1-1			
MIME-Content-Type	"application/resource-lists"		RFC 5366 [35]	PRIVATE-CALL
Resource-lists	As described in Table 5.5.3.3.1-1			
MIME-Content-Type	"application/vnd.3gpp.mcptt-location-info+xml"	This MIME part shall be included if the MCPTT-Info 'alert-ind' element sent in the MCPTT-Info is set to true.	TS 24.379 [9] clause F.3	EMERGENCY-ALERT
Location-info	As described in Table 5.5.3.4.1-1			

5.5.2.5.2 SIP INVITE from the SS

Table 5.5.2.5.2-1: SIP INVITE from the SS

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7, A.2.2.4.7				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"INVITE"			
Request-URI	px_MCPTT_Client_A_ID			
SIP-Version	"SIP/2.0"			
Via		Via header for the P-CSCF that communicates with the called party	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_PCSCF_A_URI":4060;lr"	The SS P-CSCF address and the SS protected server port		
via-branch	"z9hG4bKmcpttss1"	Value starting with 'z9hG4bK'		
Via		Via header for the other endpoint (the caller)	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Client_B_ID":14000"			
via-branch	"z9hG4bKmcpttss4"	Value starting with 'z9hG4bK'		
Record-Route		The record-route corresponding to the top Via header	RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	<sip:SS P-CSCF address: protected server port of SS;lr>		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI			
tag	"2"			
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Client_A_ID			
Call-ID			RFC 3261 [22]	
callid	px_MCPTT_CT_call_ID			
CSeq			RFC 3261 [22]	
value	"4711"			
method	"INVITE"			
Supported			RFC 3261 [22]	
option-tag	"100rel"	This option tag indicates that the UA can send or receive reliable provisional responses.		
option-tag	"timer"			
option-tag	"tdialog"			
option-tag	"norefersub"			
P-Called-Party-ID			RFC 7315 [52]	
called-pty-id-spec	px_MCPTT_Client_A_ID			
Session-Expires			RFC 4028 [30]	
generic-param	"1800"	The recommended initial value is 1800 in RFC 4028 [30].		

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7, A.2.2.4.7				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
P-Early-Media			RFC 5009 [60]	
em-parm	"inactive"			
Require			RFC 3261 [22] RFC 3312 [56] RFC 3329 [53]	
option-tag	"sec-agree"			
Proxy-Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
P-Asserted-Identity			RFC 3325 [32]	
addr-spec	px_MCPTT_User_B_ID			
Contact			RFC 3261 [22] RFC 3840 [33]	
addr-spec	px_MCPTT_Client_B_ID":14000"	SIP URI with IP address or FQDN and protected server port of the calling UE		
feature-param	"+g.3gpp.mcptt"	This media feature tag when used in a SIP request or a SIP response indicates that the function sending the SIP message supports Mission Critical Push To Talk (MCPTT) communication.	RFC 3840 [33] clause 9	
feature-param	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"	This URN indicates that the device has the capabilities to support the mission critical push to talk (MCPTT) service.	RFC 3840 [33] clause 9	
feature-param	"audio"	This feature tag indicates that the device supports audio as a streaming media type.	RFC 3840 [33] subclause 10.1	
feature-param	"isfocus"			
Max-Forwards			RFC 3261 [22]	
value	"70"	The recommended initial value is 70 in RFC 3261 [22].		
P-Access-Network-Info	Not present		RFC 7315 [52]	
access-net-specs				
Accept			RFC 3261 [22]	
media-range	"application/sdp, application/vnd.3gpp.mcptt-info+xml"			
P-Preferred-Service			RFC 6050 [31]	
Service-ID	"urn:urn-7:3gpp-service.ims.icsi.mcptt"			
P-Preferred-Identity			RFC 3325 [32]	
PPreferredID-value	px_MCPTT_User_B_ID	Contains the public user identity of the MCPTT user		
Accept-Contact			RFC 3841 [29]	
ac-value	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"			
req-param	"require"			
explicit-param	"explicit"			
Accept-Contact			RFC 3841 [29]	
ac-value	"+g.3gpp.mcptt"			
req-param	"require"			

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7, A.2.2.4.7				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
explicit-param	"explicit"			
Answer-Mode			RFC 5373 [34]	
answer-mode-value	"Auto"			
Alert-Info	Not present or Any allowed value		RFC 3261 [22], RFC 7462 [82]	
Alert-Info value				
Resource-Priority			RFC 4412 [40] RFC 7134 [57] RFC 8101 [45]	EMERGENCY-CALL or IMMPERIL-CALL
r-value	"mcpttp.value"	"value" set to the value of the <resource-priority-namespace> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration documents		EMERGENCY-CALL
r-value	"mcpttq.value"	"value" set to the value of the <resource-priority-priority> element contained in the <emergency-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document		EMERGENCY-CALL
r-value	"mcpttp.value"	"value" set to the value of the <resource-priority-namespace> element contained in the <imminent-peril-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration documents		IMMPERIL-CALL
r-value	"mcpttq.value"	"value" set to the value of the <resource-priority-priority> element contained in the <imminent-peril-resource-priority> element contained in the <OnNetwork> element of the MCPTT service configuration document		IMMPERIL-CALL
Content-Type	"multipart/mixed"		RFC 5621 [58]	
Content-Length	length of message body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/sdp"			
SDP Message	As described in Table 5.5.3.1.2-1		RFC 4566 [27]	
MIME-Content-Type	"application/vnd.3gpp.mcptt-info+xml"			

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7, A.2.2.4.7				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
MCPTT-Info	As described in Table 5.5.3.2.2-1			
MIME-Content-Type	"application/resource-lists"		RFC 5366 [35]	PRIVATE-CALL
Resource-lists	As described in Table 5.5.3.3.2-1			
MIME-Content-Type	"application/vnd.3gpp.mcptt-location-info+xml"		TS 24.379 [9] clause F.3	EMERGENCY-CALL or IMMPERIL-CALL
Location-info	As described in Table 5.5.3.4. 2-1			

5.5.2.6 SIP re-INVITE

5.5.2.6.1 SIP re-INVITE from the UE

See Table 5.5.2.5.1-1.

5.5.2.6.1 SIP re-INVITE from the SS

See Table 5.5.2.5.2-1.

5.5.2.7 SIP MESSAGE

5.5.2.7.1 SIP MESSAGE from the UE

Table 5.5.2.7.1-1: SIP MESSAGE

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7a, A.2.2.4.7a				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"MESSAGE"			
Request-URI	px_MCPTT_Server_A_URI	The public service identity identifying the originating participating MCPTT function serving the MCPTT user		
SIP-Version	"SIP/2.0″			
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID	The URI of the UE		
tag	any allowed value			
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
Call-ID			RFC 3261 [22]	
callid	any allowed value	value not checked, but stored for later reference		
Cseq			RFC 3261 [22]	
value	any allowed value			
method	"MESSAGE"			
Max-Forwards			RFC 3261 [22]	
value	any allowed value	Non-zero value		
P-Access-Network-Info			RFC 7315 [52]	
access-net-spec	any allowed value	Access network technology and, if applicable, the cell ID		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	<*sip:*SS P-CSCF address:protected server port of P-CSCF*;lr*>, <*sip:*px_scscf*;lr*>		
P-Preferred-Service			RFC 6050 [31]	
Service-ID	"urn:urn-7:3gpp-service.ims.icsi.mcptt"			
Content-Type	"multipart/mixed"		RFC 5621 [58]	
Content-Length	length of message body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/vnd.3gpp.mcptt-info+xml"		TS 24.379 [9] clause F.1	
MCPTT-Info	As described in Table 5.5.3.2.1-1			
MIME-Content-Type	"application/vnd.3gpp.mcptt-affiliation-command+xml"		TS 24.379 [9] clause F.4	
MCPPT-Affiliation-Command	As described in Table 5.5.3.7-1			
MIME-Content-Type	"application/resource-lists"		RFC 5366 [35]	PRIVATE-CALL
Resource-lists	As described in Table 5.5.3.3.1-1			

5.5.2.7.2 SIP MESSAGE from the SS

Table 5.5.2.7.2-1: SIP MESSAGE from the SS

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7a, A.2.2.4.7a				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"MESSAGE"			
Request-URI	px_MCPTT_Client_A_ID	The public service identity identifying the originating participating MCPTT function serving the MCPTT user		
SIP-Version	"SIP/2.0"			
Via		Via header for the P-CSCF that communicates with the called party	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_PCSCF_A_URI":4060;lr"	The SS P-CSCF address and the SS protected server port		
via-branch	"z9hG4bKmcpttss7"	Value starting with 'z9hG4bK'		
Via		Via header for the other endpoint (the caller)	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Client_B_ID":14000"			
via-branch	"z9hG4bKmcpttss8"	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI			
tag	"2"			
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Client_A_ID			
Call-ID			RFC 3261 [22]	
callid	px_MCPTT_CT_call_ID			
Cseq			RFC 3261 [22]	
value	"4711"			
method	"MESSAGE"			
Max-Forwards			RFC 3261 [22]	
value	"70"	The recommended initial value is 70 in RFC 3261.		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	<*sip:*SS P-CSCF address:protected server port of P-CSCF*;lr*>, <*sip:*px_scscf*;lr*>		
P-Preferred-Service			RFC 6050 [31]	
Service-ID	"urn:urn-7:3gpp-service.ims.icsi.mcptt"			

Derivation Path: TS 24.229 [16], subclause A.2.1.4.7a, A.2.2.4.7a				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Content-Type	"multipart/mixed"		RFC 5621 [58]	
Content-Length	length of message body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/vnd.3gpp.mcptt-info+xml"		TS 24.379 [9] clause F.1	
MCPTT-Info	As described in Table 5.5.3.2.1-1			
MIME-Content-Type	"application/vnd.3gpp.mcptt-affiliation-command+xml"		TS 24.379 [9] clause F.4	
MCPPT-Affiliation-Command	As described in Table 5.5.3.7-1			
MIME-Content-Type	"application/resource-lists"		RFC 5366 [35]	PRIVATE-CALL
Resource-lists	As described in Table 5.5.3.3.1-1			

5.5.2.8 SIP NOTIFY

This message is sent by the SS.

Table 5.5.2.8-1: SIP NOTIFY

Derivation Path: TS 24.229 [16] subclause A.2.1.4.8, A2.2.4.8				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22]	
Method	"NOTIFY"			
Request-URI	px_MCPTT_Client_A_ID	The URI of the UE		
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_PCSCF_A_URI":4060;lr"			
via-branch	"z9hG4bKmcpttss5"	Value starting with 'z9hG4bK'		
Via			RFC 3261 [22]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Server_A_URI":14000"	Home domain name		
via-branch	"z9hG4bKmcpttss6"	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI			
tag	same value as used in the To header of the 200 response to the SUBSCRIBE for message			
To			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	same value as received in From tag of SUBSCRIBE for message			
Call-ID			RFC 3261 [22]	
callid	same as value received in SUBSCRIBE message			
Cseq			RFC 3261 [22]	

Derivation Path: TS 24.229 [16] subclause A.2.1.4.8, A2.2.4.8				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
value	value of CSeq sent by the SS within its previous request in the same dialog but increased by one			
method	"NOTIFY"			
Contact			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn- 7:3gpp-service.ims.icsi.mcptt"			
Event			RFC 6665 [39] RFC 3842 [61]	
event-type	"presence"			
	"xcap-diff"			CONFIG GROUPCONFIG
Max-Forwards			RFC 3261 [22]	
value	"70"	The recommended initial value is 70 in RFC 3261.		
Subscription-State			RFC 6665 [39]	
substate-value	"active"			
expires	"7200"			
Content-Type	"application/pidf+xml"		RFC 3261 [22] RFC 3842 [61]	
Content-Length	length of message-body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/pidf+xml"		TS 24.379 [9] subclause 9.3.1	
PIDF	As described in Table 5.5.3.5-1			
MIME-Content-Type	"application/pidf+xml"		TS 24.379 [9] subclause 9.3.1	CONFIG
xcap_root	"uri:xcap_root.mcptt-op.gov:resource-lists"	XCAP root uri of UE configuration documents	TS 24.481 [11]	
Content-Type	"multipart/mixed"		RFC 5621 [58]	GROUPCONFIG
Content-Length	length of message body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/pidf+xml"		TS 24.379 [9] subclause 9.3.1	GROUPCONFIG
xcap_root	"uri:xcap_root.mcptt-op.gov:resource-lists"	XCAP root uri of MCPTT group configuration documents	TS 24.481 [11]	
MIME-Content-Type	"application/mikey"		RFC 3830 [24]	GROUPCONFIG
mikey	As described in Table 5.5.9.1-3	MIKEY message, containing the GSK	TS 33.179 [15]	

5.5.2.9 SIP OPTIONS

Table 5.5.2.9-1: SIP OPTIONS

Derivation Path: TS 24.229 [16] subclause A.2.1.4.9, A2.2.4.9				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Method	"OPTIONS"			
Request-Disposition	px_MCPTT_Client_A_ID			
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"			
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Server_A_URI			
Call-ID			RFC 3261 [22]	
Callid	same value as in the INVITE			
CSeq			RFC 3261 [22]	
value	value of CSeq sent by the SS within its previous request in the same dialog but increased by one			
Method	"INFO"			
Contact			RFC 3261 [22 RFC 3840 [33]	
addr-spec	"sip:[5555::aaa:bbb:ccc:eee]"	SIP URI with IP address or FQDN and protected server port of UE		
	px_MCPTT_Client_A_ID":"protected server port as chosen by the UE			
feature-param	"+g.3gpp.mcptt"	This media feature tag when used in a SIP request or a SIP response indicates that the function sending the SIP message supports Mission Critical Push To Talk (MCPTT) communication.		
feature-param	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"	This URN indicates that the device has the capabilities to support the mission critical push to talk (MCPTT) service.		
feature-param	"audio"	This feature tag indicates that the device supports audio as a streaming media type.		
Accept				
media-range	"application/sdp"			
Max-Forwards			RFC 3261 [22]	

value	any allowed value	Non-zero value		
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.10 SIP PRACK

5.5.2.10.1 SIP PRACK from the UE

Table 5.5.2.10.1-1: SIP PRACK from the UE

Derivation Path: TS 24.229 [16] subclause A.2.1.4.10, A2.2.4.10				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line			RFC 3261 [22]	
Method	"PRACK"			
Request-URI	px_MCPTT_Server_A_URI	The same URI value as the recipient of PRACK has earlier sent in its Contact header within the same dialog		
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	same value as in INVITE message			
via-branch	any allowed value	Value starting with 'z9hG4bK'		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	URIs of the Record-Route header of 183 response (or 180 when applicable) in reverse order		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"	Local tag of the dialog ID		
To			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI			
tag	"2"	Remote tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	same value as in INVITE message			
CSeq			RFC 3261 [22]	
value	value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one			
method	"PRACK"			
Max-Forwards			RFC 3261 [22]	
value	any allowed value	Non-zero value		
RAck			RFC 3261 [22]	
response-num	same value as in RSeq header of the reliable response			
cseq-num	same value as in CSeq of reliable response			
method	same value as in CSeq of reliable response			

Derivation Path: TS 24.229 [16] subclause A.2.1.4.10, A2.2.4.10				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
P-Access-Network-Info			RFC 7315 [52]	
access-net-spec	any allowed value	Access network technology and, if applicable, the cell ID		
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.10.2 SIP PRACK from the SS

Table 5.5.2.10.2-1: SIP PRACK from the SS

Derivation Path: TS 24.229 [16] subclause A.2.1.4.10, A2.2.4.10				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line			RFC 3261 [22]	
Method	"PRACK"			
Request-URI	px_MCPTT_Client_A_ID	The same URI value as the recipient of PRACK has earlier sent in its Contact header within the same dialog		
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	Same value as in INVITE message			
via-branch	"z9hG4bKmcpttss7"	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI			
tag	"1"	Local tag of the dialog ID		
To			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"2"	Remote tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	px_MCPTT_CT_call_ID			
CSeq			RFC 3261 [22]	
value	"4712"	Value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one		
method	"PRACK"			
Max-Forwards			RFC 3261 [22]	
value	"70"	The recommended initial value is 70 in RFC 3261.		
RAck			RFC 3261 [22]	
response-num	same value as in RSeq header of the reliable response			
cseq-num	same value as in CSeq of reliable response			
method	same value as in CSeq of reliable response			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.11 SIP PUBLISH

This message is sent by the UE.

Table 5.5.2.11-1: SIP PUBLISH

Derivation Path: TS 24.229 [16] subclause A.2.1.4.10A, A.2.2.4.10A				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"PUBLISH"			
Request-URI	px_MCPTT_Server_A_URI	The public service identity identifying the originating participating MCPTT function serving the MCPTT user		
SIP-Version	"SIP/2.0"			
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	<*sip:*SS P-CSCF address:protected server port of P-CSCF*;lr*>, <*sip:*px_scscf*;lr*>		
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"			
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Server_A_URI			
Expires			RFC 3261 [22] RFC 3903 [43]	
delta-seconds	"4294967295"			
Cseq			RFC 3261 [22]	
value	any allowed value			
method	"PUBLISH"			
Call-ID			RFC 3261 [22]	
callid	any allowed value			
Max-Forwards			RFC 3261 [22]	
value	any allowed value			
P-Access-Network-Info			RFC 7315 [52] RFC 7913 [51]	
access-net-spec	any allowed value	Access network technology and, if applicable, the cell ID		
Event			RFC 3903 [43]	
event-type	"presence"			
P-Preferred-Service			RFC 6050 [31]	
Service-ID	"urn:urn-7:3gpp-service.ims.icsi.mcptt"			
Accept			RFC 3261 [22]	
media-range	"application/pidf+xml"			
P-Asserted-Identity			RFC 3325 [32]	
addr-spec	px_MCPTT_User_A_ID			
Content-Type	"multipart/mixed"		RFC 5621 [58]	
Content-Length	length of message body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/vnd.3gpp.mcptt-info+xml"		TS 24.379 [9] clause F.1	
MCPTT-Info	As described in Table 5.5.3.2.1-1			

Derivation Path: TS 24.229 [16] subclause A.2.1.4.10A, A.2.2.4.10A				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
MIME-Content-Type	"application/pidf+xml"		TS 24.379 [9] subclause 9.3.1	
PIDF	As described in Table 5.5.3.5-1			
MIME-Content-Type	"application/mikey"		RFC 3830 [24]	CONFIG
mikey	As described in Table 5.5.9.1-1	MIKEY message, containing the CSK	TS 33.179 [15]	

5.5.2.12 SIP REFER

This message is sent by the UE.

Table 5.5.2.12-1: SIP REFER

Derivation Path: TS 24.229 [16] subclause A.2.1.4.11, A.2.2.4.11				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"REFER"			
Request-URI	px_MCPTT_sesson_B_ID	The session identity of the pre-established session		
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value"	IP address or FQDN and protected server port of the UE		
via-branch		Value starting with 'z9hG4bK'		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	<*sip:*SS P-CSCF address: protected server port of SS;*lr*>, <*sip:*px_scscf;*lr*>		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID	The URI of the UE		
tag	"1"	Local tag of the dialog ID		
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
tag	"2"	Remote tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	any allowed value	Value different to that received in REGISTER message		
CSeq			RFC 3261 [22]	
value	value of CSeq sent by the UE within its previous request in the same dialog but increased by one			
method	"REFER"			
P-Preferred-Identity			RFC 3325 [32]	
PPreferredID-value	px_MCPTT_User_A_ID	The public user identity		
Supported			RFC 3261 [22] RFC 6442 [62] RFC 4488 [36]	
option-tag	"norefersub"			
Refer-Sub			RFC 4488 [36]	
refer-sub-value	"false"			
Target-Dialog			RFC 4538 [37]	
callid	px_MCPTT_sesson_B_ID	The session identity of the pre-established session		
Require			RFC 3261 [22] RFC 3312 [56] RFC 3329 [53]	
option-tag	"sec-agree"			
option-tag	"multiple-refer"			
Proxy-Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Contact			RFC 3261 [22]	

Derivation Path: TS 24.229 [16] subclause A.2.1.4.11, A.2.2.4.11				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
addr-spec	"sip:[5555::aaa:bbb:ccc :eee]"	SIP URI with IP address or FQDN and protected server port of UE		
	px_MCPTT_Client_A_I D":"protected server port as chosen by the UE			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"			
feature-param	"audio"			
Refer-To			RFC 3515 [38]	
addr-spec	a Content-ID ("cid") Uniform Resource Locator (URL) as specified in IETF RFC 2392 that points to an application/resource-lists MIME body as specified in IETF RFC 5366			
Max-Forwards			RFC 3261 [22]	
value	any allowed value	Non-zero value		
P-Access-Network-Info			RFC 7315 [52]	
access-net-specs	any allowed value	Access network technology and, if applicable, the cell ID		
P-Preferred-Service			RFC 6050 [31]	
Service-ID	"urn:urn-7:3gpp-service.ims.icsi.mcptt"			
Accept-Contact		Contains the g.3gpp.icsi-ref media feature tag	RFC 3841 [29]	
ac-value	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"			
req-param	"require"			
explicit-param	"explicit"			
Accept-Contact		Contains the g.3gpp.mcptt feature tag	RFC 3841 [29]	
ac-value	"+g.3gpp.mcptt"			
req-param	"require"			
explicit-param	"explicit"			
Content-Type	"multipart/mixed"		RFC 5621 [58]	
Content-Length	length of message body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/sdp"		RFC 4566 [27]	
SDP Message	As described in Table 5.5.3.1.1-1			
MIME-Content-Type	"application/vnd.3gpp.mcptt-info+xml"		TS 24.379 [9] clause F.1	
MCPTT-Info	As described in Table 5.5.3.2.1-1			
MIME-Content-Type	"application/resource-lists"		RFC 5366 [35]	PRIVATE-CALL
Resource-lists	As described in Table 5.5.3.3.1-1			
MIME-Content-Type	"application/vnd.3gpp.mcptt-location-info+xml"		TS 24.379 [9] clause F.3	

Derivation Path: TS 24.229 [16] subclause A.2.1.4.11, A.2.2.4.11				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Location-info	As described in Table 5.5.3.4.1-1			

5.5.2.13 SIP REGISTER

This message is sent by the UE.

Table 5.5.2.13-1: SIP REGISTER

Derivation Path: TS 24.229 [16] subclause A.2.1.4.12, A.2.2.4.12				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22]	
Method	"REGISTER"			
Request-URI	px_MCPTT_Server_A_URI	The public service identity of the participating MCPTT function serving the MCPTT user		
SIP-Version	"SIP/2.0"			
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"			
To				
addr-spec	px_MCPTT_Server_A_URI			
P-Preferred-Identity			RFC 3325 [32]	
PPreferredID-value	px_MCPTT_User_A_ID			
Contact			RFC 3261 [22]	
addr-spec	"sip:[5555::aaa:bbb:ccc:eee]"	SIP URI with IP address or FQDN and protected server port of UE		
	px_MCPTT_Client_A_ID":"protected server port as chosen by the UE			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"			
feature-param	"audio"			
Accept-Contact		Contains the g.3gpp.icsi-ref media feature tag	RFC 3841 [29]	
ac-value	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"			
req-param	"require"			
explicit-param	"explicit"			
Accept-Contact		Contains the g.3gpp.mcptt feature tag	RFC 3841 [29]	
ac-value	"+g.3gpp.mcptt"			
req-param	"require"			
explicit-param	"explicit"			
P-Preferred-Service			RFC 6050 [31]	
Service-ID	'urn:urn-7:3gpp-service.ims.icsi.mcptt"			
Expires			RFC 3261 [22] RFC 3903 [43]	
value	"600000"			
Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Proxy-Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			

Supported			RFC 3261 [22] RFC 6442 [62] RFC 4488 [36]	
option-tag	"timer"			
Cseq			RFC 3261 [22]	
value	any allowed value			
method	"REGISTER"			
Session-Expires			RFC 4028 [30]	
generic-param	any allowed value			
Content-Type	"application/sdp"		RFC 3261 [22] RFC 3842 [61]	
Content-Type	"multipart/mixed"		RFC 5621 [58]	CONFIG
Content-Length	length of message-body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/sdp"		RFC 4566 [27]	
SDP Message	As described in Table 5.5.3.1.1-1			
MIME-Content-Type				CONFIG
MCPTT-Info	As described in Table 5.5.3.2.1-1			
MIME-Content-Type	"application/mikey"		RFC 3830 [24]	CONFIG
mikey	As described in Table 5.5.9.1-1	MIKEY message, containing the CSK	TS 33.179 [15]	

5.5.2.14 SIP SUBSCRIBE

This message is sent by the UE.

Table 5.5.2.14-1: SIP SUBSCRIBE

Derivation Path: TS 24.229 [16] subclause A.2.1.4.13, A.2.2.4.13				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"SUBSCRIBE"			
Request-URI	px_MCPTT_Server_A_URI	The public service identity identifying the originating participating MCPTT function serving the MCPTT user		
Request-URI	px_MCPTT_GMSURI	The configured public service identity for performing subscription proxy function of the GMS	TS 24.481 [11] subclause 6.3.13.2.1	GROUPCONFIG
SIP-Version	"SIP/2.0"			
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	<sip:SS P-CSCF address:protected server port of P-CSCF;lr>, <sip:px_scscf;lr>		
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"			
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Server_A_URI			
Contact			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID	The URI of the UE		
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref=urn:urn-7:3gpp-service.ims.icsi.mcptt"			
feature-param	"audio"			
Expires			RFC 3261 [22] RFC 3903 [43]	
value	"4294967295"			
Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Proxy-Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Cseq			RFC 3261 [22]	
value	any allowed value			
method	"SUBSCRIBE"			
Call-ID			RFC 3261 [22]	
callid	any allowed value			
Max-Forwards			RFC 3261 [22]	
value	any allowed value	Non-zero value		
P-Access-Network-Info			RFC 7315 [52] RFC 7913 [51]	

Derivation Path: TS 24.229 [16] subclause A.2.1.4.13, A.2.2.4.13				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
access-net-spec	any allowed value	Access network technology and, if applicable, the cell ID		
Event			RFC 6665 [39]	
event-type	"presence"			
	"xcap-diff"			CONFIG GROUPC ONFIG
Accept			RFC 3261 [22]	
media-range	"application/pidf+xml"			
P-Preferred-Service			RFC 6050 [31]	
Service-ID	"urn:urn-7:3gpp-service.ims.icsi.mcptt"			
P-Asserted-Identity			RFC 3325 [32]	
addr-spec	px_MCPTT_User_A_ID			
Content-Type	"multipart/mixed"		RFC 5621 [58]	
Content-Length	length of message body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/vnd.3gpp.mcptt-info+xml"		TS 24.379 [9] clause F.1	
MCPTT-Info	As described in Table 5.5.3.2.1-1			
MIME-Content-Type	"application/simple-filter+xml"		TS 24.379 [9] subclause 9.3.2	
SIMPLE-FILTER	As described in Table 5.52.22.6-1			
MIME-Content-Type	"application/resource-lists+xml"			CONFIG
Resource-lists	As described in Table 5.5.3.3.1-1			
MIME-Content-Type	"application/mikey"		RFC 3830 [24]	CONFIG
mikey	As described in Table 5.5.9.1-1	MIKEY message, containing the CSK	TS 33.179 [15]	
MIME-Content-Type	"application/resource-lists+xml"			GROUPC ONFIG
Resource-lists	As described in Table 5.5.3.3.1-1			
MIME-Content-Type	"application/mikey"		RFC 3830 [24]	GROUPC ONFIG
mikey	As described in Table 5.5.9.1-1	MIKEY message, containing the CSK	TS 33.179 [15]	

5.5.2.15 SIP UPDATE

5.5.2.15.1 SIP UPDATE from the UE

Table 5.5.2.15.1-1: SIP UPDATE from the UE

Derivation Path: TS 24.229 [16] A.2.1.4.14, A.2.2.4.14				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"UPDATE"			
Request-URI	px_MCPTT_Server_A_URI	The same URI value as the recipient of UPDATE has earlier sent in its Contact header within the same dialog		
SIP-Version	'SIP/2.0"			
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with 'z9hG4bK'		
Route			RFC 3261 [22]	
route-param	px_MCPTT_PCSCF_A_URI":4060;lr"	URIs of previous response in reverse order		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Client_A_ID	The URI of the UE		
tag	"1"	Local tag of the dialog ID		
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
tag	"2"	Remote tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	any allowed value			
Contact			RFC 3261 [22]	
addr-spec	px_MCPTT_sesson_B_ID	The URI that identifies the pre-established session		
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn- 7:3gpp-service.ims.icsi.mcptt"			
feature-param	"isfocus"			
feature-param	"audio"			
CSeq			RFC 3261 [22]	
value	any allowed value			
method	"UPDATE"			
Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Proxy-Require			RFC 3261 [22] RFC 3329 [53]	
option-tag	"sec-agree"			
Max-Forwards			RFC 3261 [22]	
value	any allowed value	Non-zero value		
P-Access-Network-Info			RFC 7315 [52] RFC 7913 [51]	
access-net-spec	any allowed value	Access network technology and, if applicable, the cell ID		
Content-Type	"application/sdp"		RFC 5621 [58]	
Content-Length	length of message-body		RFC 3261 [22]	

Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/sdp"		RFC 4566 [27]	
SDP Message	As described in Table 5.5.3.1.1-1			

5.5.2.15.2 SIP UPDATE from the SS

Table 5.5.2.15.2-1: SIP UPDATE from the SS

Derivation Path: TS 24.229 [16] A.2.1.4.14, A.2.2.4.14				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line			RFC 3261 [22] RFC 5031 [54]	
Method	"UPDATE"			
Request-URI	px_MCPTT_Client_A_ID	The same URI value as the recipient of UPDATE has earlier sent in its Contact header within the same dialog		
SIP-Version	'SIP/2.0"			
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Server_A_URI":14000"			
via-branch	"z9hG4bkmcpttss9"	Value starting with 'z9hG4bK'		
From			RFC 3261 [22]	
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
tag	"2"	Remote tag of the dialog ID		
To			RFC 3261 [22] RFC 5031 [54]	
addr-spec	px_MCPTT_Client_A_ID	The URI of the UE		
tag	"1"	Local tag of the dialog ID		
Call-ID			RFC 3261 [22]	
callid	px_MCPTT_CT_call_ID			
Contact			RFC 3261 [22]	
addr-spec	px_MCPTT_sesson_B_ID	The URI that identifies the pre-established session		
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn- 7:3gpp-service.ims.icsi.mcptt"			
feature-param	"isfocus"			
feature-param	"audio"			
CSeq			RFC 3261 [22]	
value	value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one			
method	"UPDATE"			
Max-Forwards			RFC 3261 [22]	
value	"70"	The recommended initial value is 70 in RFC 3261 [22].		
Content-Type	"application/sdp"		RFC 5621 [58]	
Content-Length	length of message-body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/sdp"		RFC 4566 [27]	
SDP Message	As described in Table 5.5.3.1.1-1			

5.5.2.16 SIP 1xx

5.5.2.16.1 SIP 100 (Trying)

This message is sent by the UE or the SS.

Table 5.5.2.16.1-1: SIP 100 (Trying)

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"100"			
Reason-Phrase	"Trying"			
Via				
via-parm	same value as received in INVITE message			
From				
addr-spec	same value as received in INVITE message			
tag	same value as received in INVITE message			
To				
addr-spec	same value as received in INVITE message			
Call-ID				
callid	same value as received in INVITE message			
CSeq				
value	same value as received in INVITE message			
Content-Length				
value	"0"	No message body included - end of SIP message		

5.5.2.16.2 SIP 180 (Ringing)

5.5.2.16.2.1 SIP 180 (Ringing) from the UE

Table 5.5.2.16.2.1-1: SIP 180 (Ringing) from the UE

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"180"			
Reason-Phrase	"Ringing"			
Record-Route				
rec-route	px_MCPTT_PCSCF_A_URI":4060;lr"	Same value as received in INVITE		
Via		Via header for the P-CSCF that communicates with the called party. same value as received in INVITE message	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_PCSCF_A_URI":4060;lr"	The SS P-CSCF address and the SS protected server port		
via-branch	"z9hG4bKmcpttss1"	Value starting with 'z9hG4bK'		
Via		Via header for the other endpoint (the caller). same value as received in INVITE message	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Client_B_ID":14000"			
via-branch	"z9hG4bKmcpttss4"	Value starting with 'z9hG4bK'		
From				
addr-spec	same value as received in INVITE message			
tag	same value as received in INVITE message			
To				
addr-spec	same value as received in INVITE message			
tag	"1"			
Contact				
addr-spec	"sip:[5555::aaa:bbb:ccc:eee]"	SIP URI with IP address or FQDN and protected server port of UE		
	px_MCPTT_Client_A_ID":"protected server port as chosen by the UE			
feature-param	"audio"			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn-7:3gpp-service.ims.icsi.mcptt"			
feature-param	"isfocus"			
Supported				
option-tag	"norefersub"			
Rseq				
response-num	previous RSeq number sent in the same direction incremented by one			
Call-ID				
callid	px_MCPTT_CT_call_ID			
CSeq				
value	"4711"			
Content-Length				

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
value	"0"	No message body included - end of SIP message		

5.5.2.16.2.2 SIP 180 (Ringing) from the SS

Table 5.5.2.16.2.1-1: SIP 180 (Ringing) from the UE

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"180"			
Reason-Phrase	"Ringing"			
Record-Route				
rec-route	px_MCPTT_PCSCF_A_URI":4060;lr"	Same value as received in INVITE		
Via			RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	same value as received in INVITE	IP address or FQDN and protected server port of the UE		
via-branch	same value as received in INVITE	Value starting with 'z9hG4bK'		
From				
addr-spec	same value as received in INVITE message			
tag	"1"			
To				
addr-spec	same value as received in INVITE message			
tag	"2"			
Contact				
addr-spec	px_MCPTT_Client_B_ID":14000"	px_CalleeContactUri		
feature-param	"audio"			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn-7:3gpp-service.ims.icsi.mcptt"			
feature-param	"isfocus"			
Supported				
option-tag	"norefersub"			
Rseq				
response-num	previous RSeq number sent in the same direction incremented by one			
Call-ID				
callid	same value as received in INVITE message			
CSeq				
value	same value as received in INVITE message			
Content-Length				
value	"0"	No message body included - end of SIP message		

5.5.2.16.3 SIP 183 (Session Progress)

5.5.2.16.3.1 SIP 183 (Session Progress) from the UE

Table 5.5.2.16.3.1-1: SIP 183 (Session Progress) from the UE

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"183"			
Reason-Phrase	"Session progress"			
Record-Route				
rec-route	px_MCPTT_PCSCF_A_URI":4060;lr"	Same value as received in INVITE		
Via		Via header for the P-CSCF that communicates with the called party. same value as received in INVITE message	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_PCSCF_A_URI":4060;lr"	The SS P-CSCF address and the SS protected server port		
via-branch	"z9hG4bKmcpttss1"	Value starting with 'z9hG4bK'		
Via		Via header for the other endpoint (the caller). same value as received in INVITE message	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Client_B_ID":14000"			
via-branch	"z9hG4bKmcpttss4"	Value starting with 'z9hG4bK'		
Require				
option-tag	"100rel"			
From				
addr-spec	same value as received in INVITE message			
tag	same value as received in INVITE message			
To				
addr-spec	same value as received in INVITE message			
tag	"1"			
Contact				
addr-spec	"sip:[5555::aaa:bbb:ccc:eee]"	SIP URI with IP address or FQDN and protected server port of UE		
	px_MCPTT_Client_A_ID":"protected server port as chosen by the UE			
feature-param	"audio"			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn-7:3gpp-service.ims.icsi.mcptt"			
feature-param	"isfocus"			
Supported				
option-tag	"norefersub"			
Rseq				
response-num	previous RSeq number sent in the same direction incremented by one			
Call-ID				
callid	px_MCPTT_CT_call_ID	Same value as received in INVITE message		

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
CSeq				
value	"4711"	Same value as received in INVITE message		
P-Answer-State		optional		
value	"unconfirmed"			
P-Asserted-Identity			RFC 3325 [32]	
addr-spec	px_MCPTT_User_A_ID	The URI of the UE		
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.16.3.2 SIP 183 (Session Progress) from the SS

Table 5.5.2.16.3.2-1: SIP 183 (Session Progress) from the SS

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"183"			
Reason-Phrase	"Session progress"			
Record-Route				
rec-route	px_MCPTT_PCSCF_A_URI":4060;lr"	Same value as received in INVITE		
Via		Via header for the P-CSCF that communicates with the called party. same value as received in INVITE message	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	same value as received in INVITE	IP address or FQDN and protected server port of the UE		
via-branch	same value as received in INVITE	Value starting with 'z9hG4bK'		
Require				
option-tag	"100rel"			
From				
addr-spec	same value as received in INVITE message			
tag	"1"			
To				
addr-spec	same value as received in INVITE message			
tag	"2"			
Contact				
addr-spec	px_MCPTT_Client_B_ID":14000"	px_CalleeContactUri		
feature-param	"audio"			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn-7:3gpp-service.ims.icsi.mcptt"			
feature-param	"isfocus"			
Supported				
option-tag	"norefersub"			
Rseq				
response-num	previous RSeq number sent in the same direction incremented by one			
Call-ID				
callid	same value as received in INVITE message			
CSeq				
value	same value as received in INVITE message			
P-Answer-State				
value	"unconfirmed"			
P-Asserted-Identity			RFC 3325 [32]	
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.17 SIP 2xx

5.5.2.17.1 SIP 200 (OK)

5.5.2.17.1.1 SIP 200 (OK) from the UE

Table 5.5.2.17.1.1-1: SIP 200 (OK) from the UE

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"200"			
Reason-Phrase	"OK"			
Via		Via header for the P-CSCF that communicates with the called party. same value as received in INVITE message	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_PCSCF_A_URI":4060;lr"	The SS P-CSCF address and the SS protected server port		
via-branch	"z9hG4bKmcpttss1"	Value starting with 'z9hG4bK'		
Via		Via header for the other endpoint (the caller). same value as received in INVITE message	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	px_MCPTT_Client_B_ID":14000"			
via-branch	"z9hG4bKmcpttss4"	Value starting with 'z9hG4bK'		
Record-Route				
rec-route	px_MCPTT_PCSCF_A_URI":4060;lr"			
From				
addr-spec	px_MCPTT_Server_A_URI			
tag	"2"			
To				
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"			
P-Asserted-Identity				
addr-spec	px_MCPTT_Server_A_URI			
Contact				
addr-spec	px_MCPTT_Server_A_URI			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn- 7:3gpp-service.ims.icsi.mcptt"			
feature-param	"isfocus"			
feature-param	"audio"			
Call-ID				
callid	px_MCPTT_CT_call_ID			
CSeq				
value	"4711"			
Require				
option-tag	"timer"			
Session-Expires				
generic-param	"3600"			
refresher	"uac"			
Supported				
option-tag	"tdialog"			
option-tag	"norefersub"			
option-tag	"explicitsub"			
option-tag	"nosub"			
Content-Type	"application/sdp"		RFC 5621 [58]	

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Content-Length	length of message-body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/sdp"		RFC 4566 [27]	
SDP Message	As described in Table 5.5.3.1.1-1			

5.5.2.17.1.2 SIP 200 (OK) from the SS

Table 5.5.2.17.1.2-1: SIP 200 (OK) from the SS

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"200"			
Reason-Phrase	"OK"			
Via		Via header for the P-CSCF that communicates with the called party. same value as received in INVITE message	RFC 3261 [22] RFC 3581 [55]	
sent-protocol	"SIP/2.0/UDP"			
sent-by	same value as received in INVITE	IP address or FQDN and protected server port of the UE		
via-branch	same value as received in INVITE	Value starting with 'z9hG4bK'		
Record-Route				
rec-route	px_MCPTT_PCSCF_A_URI":4060;lr"	Same value as received in INVITE		
From				
addr-spec	px_MCPTT_Client_A_ID			
tag	"1"			
To				
addr-spec	px_MCPTT_Server_A_URI			
tag	"2"			
P-Asserted-Identity				
addr-spec	px_MCPTT_User_A_ID			
Contact				
addr-spec	px_MCPTT_Client_A_ID			
feature-param	"+g.3gpp.mcptt"			
feature-param	"+g.3gpp.icsi-ref= urn:urn- 7:3gpp-service.ims.icsi.mcptt"			
feature-param	"isfocus"			
feature-param	"audio"			
Call-ID				
callid	same value as received in INVITE message			
CSeq				
value	same value as received in INVITE message			
Require				
option-tag	"timer"			
Session-Expires				
generic-param	"3600"			
refresher	"uac"			
Supported				
option-tag	"tdialog"			
option-tag	"norefersub"			
option-tag	"explicitsub"			
option-tag	"nosub"			
Feature-Caps	Not Present or Any allowed value		RFC 6809 [81]	
fcap-name				
Content-Type	"application/sdp"		RFC 5621 [58]	
Content-Length	length of message-body		RFC 3261 [22]	
Message-body			RFC 3261 [22]	
MIME-Content-Type	"application/sdp"		RFC 4566 [27]	
SDP Message	As described in Table 5.5.3.1.1-1			

5.5.2.18 SIP 3xx

5.5.2.18.1 SIP 302 (Moved Temporarily)

Table 5.5.2.18.1-1: SIP 302 (Moved Temporarily)

Delivery Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"302"			
Reason-Phrase	"Moved Temporarily"			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.19 SIP 4xx

5.5.2.19.1 SIP 403 (Forbidden)

Table 5.5.2.19.1-1: SIP 403 (Forbidden)

Delivery Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"403"			
Reason-Phrase	"Forbidden"			
Warning				
mcptt-warn-code	"100"			
mcptt-warn-text	"function not allowed due to" <detailed reason>			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.19.2 SIP 404 (Not Found)

Table 5.5.2.19.2-1: SIP 404 (Not Found)

Delivery Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"404"			
Reason-Phrase	"Not Found"			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.19.3 SIP 423 (Interval Too Brief)

Table 5.5.2.19.3-1: SIP 423 (Interval Too Brief)

Delivery Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"423"			
Reason-Phrase	"Internal Too Brief"			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.19.4 SIP 480 (Temporarily unavailable)

This message is sent by the UE.

Table 5.5.2.19.4-1: SIP 480 (Temporarily unavailable)

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"480"			
Reason-Phrase	"Temporarily Unavailable"			
Via				
sent-protocol	"SIP/2.0/UDP"			
sent-by	any allowed value	IP address or FQDN and protected server port of the UE		
via-branch	any allowed value	Value starting with 'z9hG4bK'		
From				
addr-spec	px_MCPTT_Client_A_ID	The URI of the UE		
tag	"1"			
To				
addr-spec	px_MCPTT_Server_A_URI	The URI of the SS		
tag	"2"			
Warning				
warn-code	"110"			
warn-text	"user declined the call invitation"			
Call-ID				
callid	px_MCPTT_CT_call_ID			
CSeq				
value	"4711"			
method	"INVITE"			
Content Length				
value	"0"	No message body included - end of SIP message		

5.5.2.19.5 SIP 486 (Busy Here)

Table 5.5.2.19.5-1: SIP 486 (Busy Here)

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"486"			
Reason-Phrase	"Busy Here"			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.19.6 SIP 488 (Not Acceptable Here)

Table 5.5.2.19.6-1: SIP 488 (Not Acceptable Here)

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"488"			
Reason-Phrase	"Not Acceptable Here"			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.19.6 SIP 401 (Unauthorized)

Table 5.5.2.19.6-1: SIP 488 (Not Acceptable Here)

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"488"			
Reason-Phrase	"Not Acceptable Here"			
WWW-Authenticate				
realm	px_MCPTT_User_A_Organization			
algorithm	"AKAv1-MD5"			
qop-value	"auth"			
nonce	Base 64 encoding of RAND and AUTN			
opaque	arbitrary value (to be returned by the UE in subsequent REGISTER)			
Security-Server				
mechanism-name	"ipsec-3gpp"			
algorithm	px_IpSecAlgorithm (hmac-md5-96 or hmac-sha-1-96)			
spi-c	SPI number of the inbound SA at the protected client port			
spi-s	SPI number of the inbound SA at the protected server port			
port-c	protected client port of SS			
port-s	protected server port of SS			
Encrypt-algorithm	des-ede3-cbc or aes-cbc			
q	"0.9"			
Mechanism-name	"Ipsec-3gpp"			
algorithm	Algorithm not selected by px_IpSecAlgorithm (hmac-sha-1-96 or hmac-md5-96)			
spi-c	SPI number of the inbound SA at the protected client port			
spi-s	SPI number of the inbound SA at the protected server port			
port-c	protected client port of SS			
port-s	protected server port of SS			
encrypt-algorithm	des-ede3-cbc or aes-cbc			
q	"0.7"			
Content-length	"0"			

5.5.2.20 SIP 5xx

5.5.2.20.1 SIP 500 (Server Internal Error)

Table 5.5.2.20.1-1: SIP 500 (Server Internal Error)

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"500"			
Reason-Phrase	"Server Internal Error"			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.2.21 SIP 6xx

5.5.2.21.1 SIP 606 (Not Acceptable)

Table 5.5.2.21.1-1: SIP 606 (Not Acceptable)

Derivation Path: RFC 3261 [22]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
SIP-Version	"SIP/2.0"			
Status-Code	"606"			
Reason-Phrase	"Not Acceptable"			
Content-Length			RFC 3261 [22]	
value	"0"	No message body included - end of SIP message		

5.5.3 Default SDP message and other information elements

5.5.3.1 SDP Message

5.5.3.1.1 SDP Message from the UE

Table 5.5.3.1.1-1: SDP Message from the UE

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Session description:				
Protocol Version	"0"	v= line		
Origin		o= line		
username	px_MCPTT_User_A_ID	Username of client		
sess-id	any allowed value	A numeric string such that the tuple of <username>, <sess-id>, <nettype>, <addrtype>, and <unicast-address> forms a globally unique identifier for the session.		
sess-version	any allowed value			
nettype	"IN"			
addrtype	"IP4"	"IP4" or "IP6"		
unicast-address	px_MCPTT_IP_ConnectionAddressAll			
Session Name	at least one UTF-8-encoded character, or if no name is given, a single empty space	s= line		
Connection Data	not required if included in all media	c= line Included if the media plane control channel uses a different IP address than other media described in the SDP		
nettype	"IN"			
addrtype	"IP4"	"IP4" or "IP6"		
connection-address	px_MCPTT_IP_ConnectionAddressAll			
Bandwidth		b= line		
bwtype	"AS:"	bwtype:bandwidth		
bandwidth	any allowed value		TS 26.114 [64] Table K.6	
Time description				
Timing		t= line		
start-time	"0"			
stop-time	"0"			
Media descriptions				
media description		m= line media = audio	RFC 4867 [59]	
media	"audio"			
port	any allowed value	The transport port to which the media stream is sent		
proto	"RTP/AVP"			
fmt	any allowed value(s)	Indicating RTP payload type numbers		
media title	"speech"	i= line		
Connection Data		c= line Included if the media plane for audio uses a different IP address than other media described in the SDP		
nettype	"IN"			
addrtype	"IP4"			
connection-address	px_MCPTT_IP_ConnectionAddressAudio			
media attribute		a= line attribute = rtpmap		
rtpmap	"rtpmap"			

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
payload type	"99"			
encoding name	"AMR-WB"			
clock rate	16000		RFC 4867 [59] subclause 8.3	
encoding parameter	"1" if present	Channel number		
media attribute		a= line attribute = fmtp		
fmtp	"fmtp"			
format	the value given in fmt in the audio media description			
format specific parameters		Parameters of WB-AMR codec		
mode-change-capability	"2"	To be able to interoperate fully with gateways to circuit switched networks	RFC 4867 [59] subclause 8.2	
max-red	"0"	No redundancy will be used	RFC 4867 [59] subclause 8.2	
media attribute		a= line attribute =ptime		
ptime	any allowed value	packet time		
media attribute		a= line attribute =maxptime		
maxptime	any allowed value	maximum packet time		
media description		m= line media = application SDP media-level section for a media-floor control entity		
media	"application"			
port	any allowed value	The port for the media-floor control entity		
proto	"udp"			
fmt	"MCPTT"			
Connection Data		c= line Included if the media plane control channel uses a different IP address than other media described in the SDP		
nettype	"IN"			
addrtype	"IP4"			
connection-address	px_MCPTT_IP_ConnectionAddressApp			
media attribute		a= line attribute = fmtp		
fmtp				
format	"MCPTT"			
format specific parameters				
mc_queueing	optional	Parameter has no value	TS 24.380 [10] cl. 12.1.2.3	
mc_priority	not present or any allowed value	Any integer value in the range of 1..255	TS 24.380 [10] cl. 12.1.2.3	
mc_granted	present	Parameter has no value	TS 24.380 [10] cl. 12.1.2.3	
mc_implicit_request	present	Parameter has no value	TS 24.380 [10] cl. 12.1.2.3	
media attribute		a= line attribute = key-mgmt		PRIVATE-CALL

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
key-mgmt			TS 24.379 [9] subclause 6.2.1	
mikey	MIKEY-SAKKE I_MESSAGE as specified in Table 5.5.9.1-2		RFC 4567 [44]	

5.5.3.1.2 SDP Message from the SS

Table 5.5.3.1.2-1: SDP Message from the SS

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Session description:				
Protocol Version	"0"	v= line		
Origin		o= line		
username	px_MCPTT_User_B_ID	Username of client sending message		
sess-id	"12345678"	A numeric string such that the tuple of <username>, <sess-id>, <nettype>, <addrtype>, and <unicast-address> forms a globally unique identifier for the session.		
sess-version	"12345678"			
nettype	"IN"			
addrtype	"IP4"	This depends on the unicast address of the UE		
unicast-address	px_MCPTT_IP_ConnectionAddressAll			
Session Name	at least one UTF-8-encoded character, or if no name is given, a single empty space	s= line		
Bandwidth		b= line		
bwtype	"AS:"	bwtype:bandwidth		
bandwidth	"38"	kilobits per second; Maximum AMR-WB at 23.85 kbps but limit to 12.65 kbps plus overhead	TS 26.114 [64] Table K.6	
Time description				
Timing		t= line		
start-time	"0"			
stop-time	"0"			
Media descriptions				
media description		m= line media = audio	RFC 4867 [59]	
media	"audio"			
port	"49152"	The transport port to which the media stream is sent	RFC 6335 [63] subclause 6	
proto	"RTP/AVP"			
fmt	"99"	RTP/AVP payload type for AMR-WB is dynamic		
media title	"speech"	i= line		
Connection Data		c= line		
nettype	"IN"			
addrtype	"IP4"	This depends on the connection address		
connection-address	px_MCPTT_IP_ConnectionAddressAudio			
media attribute		a= line attribute = rtpmap		
rtpmap	"rtpmap"			
payload type	"99"			
encoding name	"AMR-WB"			
clock rate	16000		RFC 4867 [59] subclause 8.3	
encoding parameter	"1" if present	Channel number		
media attribute		a= line attribute = fmtp		
fmtp				

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
format	"99"			
format specific parameters		Parameters of WB-AMR codec		
mode-change-capability	"2"	To be able to interoperate fully with gateways to circuit switched networks	RFC 4867 [59] subclause 8.2	
max-red	"0"	No redundancy will be used	RFC 4867 [59] subclause 8.2	
media attribute		a= line attribute =ptime		
ptime	"20"	packet time		
media attribute		a= line attribute =maxptime		
maxptime	"240"	maximum packet time		
media description		m= line media = application SDP media-level section for a media-floor control entity		
media	"application"			
port	"49153"	The port for the media-floor control entity		
proto	"udp"			
fmt	"MCPTT"			
Connection Data		c= line		
nettype	"IN"			
addrtype	"IP4"	This depends on the connection address		
connection-address	px_MCPTT_IP_ConnectionAddressApp			
media attribute		a= line attribute = fmtp		
fmtp				
format	"MCPTT"			
format specific parameters				
mc_queueing	Present	Parameter has no value	TS 24.380 [10] cl. 12.1.2.3	
mc_priority	"5"	Any integer value in the range of 1..255	TS 24.380 [10] cl. 12.1.2.3	
mc_granted	Present	Parameter has no value	TS 24.380 [10] cl. 12.1.2.3	
mc_implicit_request	Present	Parameter has no value	TS 24.380 [10] cl. 12.1.2.3	
media attribute		a= line attribute = key-mgmt		PRIVATE-CALL
key-mgmt			TS 24.379 [9] subclause 6.2.1	
mikey	MIKEY-SAKKE I_MESSAGE as specified in Table 5.5.9.1-2		RFC 4567 [44]	

5.5.3.1.3 SDP Message from the UE - Off-network

Table 5.5.3.1.3-1: SDP Message from the UE - Off-network

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Session description:				
Protocol Version	"0"	v= line		
Origin		o= line		
username	"-"			
sess-id	any allowed value	A numeric string such that the tuple of <username>, <sess-id>, <nettype>, <addrtype>, and <unicast-address> forms a globally unique identifier for the session.		
sess-version	any allowed value			
nettype	"IN"			
addrtype	"IP4"	"IP4" or "IP6"		
unicast-address	px_MCPTT_IP_ConnectionAddressAll			
Session Name	"-"	s= line		
Connection Data		c= line		
nettype	"IN"			
addrtype	"IP4"	"IP4" or "IP6"		
connection-address	px_MCPTT_IP_ConnectionAddressAll	Set to the multicast IP address of the MCPTT group		
Bandwidth		b= line		
bwtype	"AS:"	bwtype:bandwidth		
bandwidth	any allowed value			
Time description				
Timing		t= line		
start-time	"0"			
stop-time	"0"			
Media descriptions				
media description		m= line media = audio		
media	"audio"			
port	any allowed value	Set to a port number for MCPTT speech of the MCPTT group		
proto	"RTP/AVP"			
fmt	any allowed value(s)	Indicating RTP payload type numbers		
media title	"speech"	i= line		
media attribute		a= line attribute = rtpmap		
rtpmap	"rtpmap"			
payload type	"99"			
encoding name	"AMR-WB"			
clock rate	16000			
encoding parameter	"1" if present	Channel number		
media attribute		a= line attribute = fmtp		
fmtp	"fmtp"			
format	the value given in fmt in the audio media description			
format specific parameters		Parameters of WB-AMR codec		
mode-change-capability	"2"	To be able to interoperate fully with gateways to circuit switched networks		
max-red	"0"	No redundancy will be used		

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
media attribute		a= line attribute =ptime		
ptime	any allowed value	packet time		
media attribute		a= line attribute =maxptime		
maxptime	any allowed value	maximum packet time		
media description		m= line media = application		
media	"application"			
port	any allowed value	Set to a port number for media-floor control entity of the MCPTT group		
proto	"udp"			
fmt	"MCPTT"			
media attribute		a= line attribute = fmtp		
fmtp				
format	"MCPTT"			
format specific parameters				
mc_queueing	optional	Parameter has no value		
mc_priority	not present or any allowed value	Any integer value in the range of 1..255		
mc_granted	present	Parameter has no value		
mc_implicit_request	present	Parameter has no value		
media attribute		a= line attribute = key-mgmt		
key-mgmt				
mikey	MIKEY-SAKKE I_MESSAGE as specified in Table 5.5.9.1-2			

5.5.3.1.4 SDP Message from the SS - Off-network

Table 5.5.3.1.4-1: SDP Message from the SS - Off-network

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Session description:				
Protocol Version	"0"	v= line		
Origin		o= line		
username	"-"			
sess-id	"12345678"	A numeric string such that the tuple of <username>, <sess-id>, <nettype>, <addrtype>, and <unicast-address> forms a globally unique identifier for the session.		
sess-version	"12345678"			
nettype	"IN"			
addrtype	"IP4"			
unicast-address	px_MCPTT_IP_ConnectionAddressAll			
Session Name	"-"	s= line		
Connection Data		c= line		
nettype	"IN"			
addrtype	"IP4"	"IP4" or "IP6"		
connection-address	px_MCPTT_IP_ConnectionAddressAll	Set to the multicast IP address of the MCPTT group		
Bandwidth		b= line		
bwtype	"AS:"	bwtype:bandwidth		
bandwidth	any allowed value			
Time description				
Timing		t= line		
start-time	"0"			
stop-time	"0"			
Media descriptions				
media description		m= line media = audio		
media	"audio"			
port	"49152"	Set to a port number for MCPTT speech of the MCPTT group		
proto	"RTP/AVP"			
fmt	"99"	Indicating RTP payload type numbers		
media title	"speech"	i= line		
media attribute		a= line attribute = rtpmap		
rtpmap	"rtpmap"			
payload type	"99"			
encoding name	"AMR-WB"			
clock rate	16000			
encoding parameter	"1" if present	Channel number		
media attribute		a= line attribute = fmtp		
fmtp	"fmtp"			
format	"99"			
format specific parameters		Parameters of WB-AMR codec		
mode-change-capability	"2"	To be able to interoperate fully with gateways to circuit switched networks		
max-red	"0"	No redundancy will be used		
media attribute		a= line attribute =ptime		

Derivation Path: RFC 4566 [27]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
ptime	"20"	packet time		
media attribute		a= line attribute =maxptime		
maxptime	"240"	maximum packet time		
media description		m= line media = application		
media	"application"			
port	"49153"	Set to a port number for media-floor control entity of the MCPTT group		
proto	"udp"			
fmt	"MCPTT"			
media attribute		a= line attribute = fmtp		
fmtp				
format	"MCPTT"			
format specific parameters				
mc_queueing	Present	Parameter has no value		
mc_priority	"5"	Any integer value in the range of 1..255		
mc_granted	Present	Parameter has no value		
mc_implicit_request	Present	Parameter has no value		
media attribute		a= line attribute = key-mgmt		
key-mgmt				
mikey	MIKEY-SAKKE I_MESSAGE as specified in Table 5.5.9.1-2			

5.5.3.2 MCPTT-Info

5.5.3.2.1 MCPTT-Info from the UE

Table 5.5.3.2.1-1: MCPTT-Info from the UE

Derivation Path: TS 24.379 [9] subclause F.1.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
mcpttinfo				
mcptt-Params				
mcptt-access-token	not present			
	"eyJhbGciOiJSUzI1NiJ9.eyJtY3B0dF9pZCI6ImFsaWNlQG9yZy5jb20iLCJleHAiOjE0NTM1MDYxMjEsInNjb3BlIjpbIm9wZW5pZCIsIjNncHA6bWNwdHQ6cHR0X3NlcnZlciJdLCJjbGllbnRfaWQiOiJtY3B0dF9jbGllbnQifQ.XYIqai4YKSZCKRNMLipGC_5nV4BE79IJpvjexWjIqqcqiEx6AmHHIRo0mhcxeCESrXei9krom9e8Goxr_hgF3szvgbwl8JRbFuv97XgepDLjEq4jL3Cbu41Q9b0WdXAdFmeEbiB8wo_xggiGwv6IDR1b3TgAAsdjkRxSK4ctIKPaOJSRmM7MKMcKhIug3BEkSC9-aXBTSIv5fAGN-ShDbPvHycBpjzKWXBvMIR5PaCg-9fwjELXZXdRwz8C6JbRM8aqzhdt4CVhQ3-Arip-S9CKd0tu-qhHfF2rvJDRlg8ZBiihdPH8mJs-qpTFep_1-kON3mL0_g54xVmlMwN0XQA"	The access token is opaque to the MCPTT client	TS 33.179 [15], clause B.3 RFC 6749 [77]	CONFIG
session-type	"prearranged"			GROUP-CALL
	"private"			PRIVATE-CALL
mcptt-request-uri	px_MCPTT_Group_A_ID	The URI of the group		GROUP-CALL
	px_MCPTT_Client_B_ID	The URI of the invited MCPTT Client		PRIVATE-CALL
mcptt-calling-user-id	not present or px_MCPTT_User_A_ID			
mcptt-called-party-id	not present or px_MCPTT_User_B_ID			
mcptt-calling-group-id	not present			
required	not present			
emergency-ind	not present or if present then="false"			
	"true"			EMERGENCY-CALL
alert-ind	not present or if present then="false"			
	"true"			EMERGENCY-ALERT
imminentperil-ind	not present or if present then="false"			
	"true"			IMMPERIL-CALL
broadcast-ind	not present			
mc-org"	not present			
floor-state	not present			

Derivation Path: TS 24.379 [9] subclause F.1.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
associated-group-id	px_MCPTT_Group_A_ID if mcptt-request-uri contains a temporary group identity; otherwise, not present	if the <mcptt-request-uri> element contains a group identity then this element can include an MCPTT group ID associated with the group identity in the <mcptt-request-uri> element. E.g. if the <mcptt-request-uri> element contains a temporary group identity (TGI), then the <associated-group-id> element can contain the constituent MCPTT group ID	TS 24.379 [9] subclause F.1.3	GROUP-CALL
	not present			PRIVATE-CALL
originated-by	not present			
MKFC-GKTPs	not present			
mcptt-client-id	px_MCPTT_Client_A_ID	The URI of the MCPTT Client		PRIVATE-CALL GROUP-CALL EMERGENCY-CALL IMMPERIL-CALL EMERGENCY-ALERT
	"eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiYXVkIjoibWNwdHRfY2xpZW50IiwiaXNzIjoiSWRNUy5zZXJ2ZXIuY29tOjkwMzEiLCJpYXQiOjE0NTM0OTgxNTgsImV4cCI6MTQ1MzQ5ODQ1OCwibWNwdHRfaWQiOiJhbGljZUBvcmcuY29tIn0.Dpn7AhIMaqMEgg12NYUUfJGSFJMPG8M2li9FLtPotDlHvwU2emBws8z5JLw81SXQnoLqZ8ZF8tIhZ1W7uuMbufF4Wsr7PAadZixz3CnV2wxFV9qR_VA1-0ccDTPukUsRHsic0SgZ3aIbcYKd6VsehFe_GDwfqysYzD7yPwCfPZo"	The MCPTT client may validate the user with the ID token and configure itself for the user	TS 33.179 [15], clause B.3 RFC 6749 [77]	CONFIG
alert-ind-rcvd	not present			
anyExt	not present or any allowed value		TS 24.379 [9], subclause F.1.3	

5.5.3.2.2 MCPTT-Info from the SS

Table 5.5.3.2.2-1: MCPTT-Info from the SS

Derivation Path: TS 24.379 [9] subclause F.1.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
mcpttinfo				
mcptt-Params				
mcptt-access-token	not present			
session-type	"prearranged"			GROUP-CALL
	"private"			PRIVATE-CALL
mcptt-request-uri	px_MCPTT_User_A_ID	The URI of the called user		
mcptt-calling-user-id	px_MCPTT_User_B_ID	The URI of the calling user		
mcptt-called-party-id	not present			
mcptt-calling-group-id	px_MCPTT_Group_A_ID	The URI of the group		GROUP-CALL
	not present			PRIVATE-CALL
required	not present			
emergency-ind	not present			
	"true"			EMERGENCY-CALL
alert-ind	not present			
	"true"			EMERGENCY-ALERT
imminentperil-ind	not present			
	"true"			IMMPERIL-CALL
broadcast-ind	not present			
mc-org"	not present			
floor-state	not present			
associated-group-id	not present			
originated-by	not present			
MKFC-GKTPs	not present			
mcptt-client-id	not present			
alert-ind-rcvd	not present			
anyExt	not present or any allowed value		TS 24.379 [9], subclause F.1.3	

5.5.3.3 Resource-lists

5.5.3.3.1 Resource-lists from the UE

Table 5.5.3.3.1-1: Resource-lists from the UE

Derivation Path: RFC 5366 [35] / RFC 4826 [83]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
resource-lists				PRIVATE-CALL GROUP-CALL EMERGENCY-CALL IMMPERIL-CALL EMERGENCY-ALERT
resource-lists	"uri: mcptt-op.gov:resource-lists"		TS 24.481 [11]	CONFIG
list				
entry	px_MCPTT_User_B_ID	The MCPTT ID of the invited user		PRIVATE-CALL GROUP-CALL EMERGENCY-CALL IMMPERIL-CALL EMERGENCY-ALERT
entry	"resource-lists/ue_configuration.xml/"	UE Configuration document	TS 24.481 [11]	CONFIG
entry	"resource-lists/ue_user_profile.xml/"	UE User Profile document	TS 24.481 [11]	CONFIG
entry	"resource-lists/ue_service_configuration.xml/"	UE Service Configuration document	TS 24.481 [11]	CONFIG
entry	"resource-lists/ue_group_configuration.xml/"	UE Group Configuration document	TS 24.481 [11]	GROUPCONFIG

5.5.3.3.2 Resource-lists from the SS

Table 5.5.3.3.2-1: Resource-lists from the SS

Derivation Path: RFC 5366 [35] / RFC 4826 [83]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
resource-lists				
list				
entry	px_MCPTT_User_A_ID	The MCPTT ID of the invited user		

5.5.3.4 Location-info

5.5.3.4.1 Location-info (Report from the UE)

Table 5.5.3.4.1-1: Location-info (Report from the UE)

Derivation Path: TS 24.379 [9] clause F.3				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
location-info				
Report				
TriggerID	not present	An element which can occur multiple times. Contains the value of the <TriggerId> attribute associated with a trigger that has fired. Only present if a trigger is the cause of the Location-info Report.		
CurrentLocation		A mandatory element that contains the location information		
CurrentServingEcgi	optional	This is optional depending on the configuration sent by the SS		
NeighbouringEcgi	optional	This is optional depending on the configuration sent by the SS		
MbmsSaId	optional	This is optional depending on the configuration sent by the SS		
MbsfnArea	optional	This is optional depending on the configuration sent by the SS		
CurrentCoordinate	optional	This is optional depending on the configuration sent by the SS		
ReportID	not present	Attribute is used to return the value in the <RequestId> attribute in the <Request> element. Only present in response to a Location-Info Request.		
ReportType	"Emergency"	Required The <ReportType> attribute has two values "Emergency" and "NonEmergency" used to inform whether the client is sending the report in an emergency situation or not.		
EmergencyEventType	"GroupCallEmergency"			GROUP-CALL and EMERGENCY-CALL
	"GroupCallImminentPeril"			GROUP-CALL and IMMPERIL-CALL
	"PrivateCallEmergency"			PRIVATE-CALL and EMERGENCY-CALL

Derivation Path: TS 24.379 [9] clause F.3				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
	"InitiateEmergencyAlert"			IMMPERIL-CALL

5.5.3.4.2 Location-info (Configuration sent by the SS)

Table 5.5.3.4.2-1: Location-info (Configuration sent by the SS)

Derivation Path: TS 24.379 [9] clause F.3				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
location-info				
Configuration				
ConfigScope	"Full"	The MCPTT Client shall replace any previous configuration.		
NonEmergencyLocationInformation				
ServingEcgi	present	An optional element specifying that the serving E-UTRAN Cell Global Identity (ECGI) needs to be reported		
NeighbouringEcgi	present	An optional element that can occur multiple times, specifying that neighbouring ECGIs need to be reported		
MbmsSaId	present	An optional element specifying that the serving MBMS Service Area Id needs to be reported;		
MbsfnArea	present	An optional element specifying that the MBSFN area Id needs to be reported;		
GeographicalCoordinate	present	An optional element specifying that the geographical coordinate specified in subclause 6.1 in 3GPP TS 23.032 [65] needs to be reported		
minimumIntervalLength	"10"	A mandatory element specifying the minimum time the MCPTT client needs to wait between sending location reports. The value is given in seconds		
EmergencyLocationInformation"				
ServingEcgi	present	An optional element specifying that the serving E-UTRAN Cell Global Identity (ECGI) needs to be reported		
NeighbouringEcgi	present	An optional element that can occur multiple times, specifying that neighbouring ECGIs need to be reported		
MbmsSaId	present	An optional element specifying that the serving MBMS Service Area Id needs to be reported;		
MbsfnArea	present	An optional element specifying that the MBSFN area Id needs to be reported;		

Derivation Path: TS 24.379 [9] clause F.3				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
GeographicalCoordinate	present	An optional element specifying that the geographical coordinate specified in subclause 6.1 in 3GPP TS 23.032 [65] needs to be reported		
minimumIntervalLength	"5"	A mandatory element specifying the minimum time the MCPTT client needs to wait between sending location reports. The value is given in seconds		
TriggeringCriteria				
CellChange	not present			
TrackingAreaChange	not present			
PlmnChange	not present			
MbmsSaChange	not present			
MbsfnAreaChange	not present			
PeriodicReport	not present			
TravelledDistance	not present			
McpttSignallingEvent	not present			
GeographicalAreaChange	not present			

5.5.3.4.3 Location-info (Request sent by the SS)

Table 5.5.3.4.3-1: Location-info (Request sent by the SS)

Derivation Path: TS 24.379 [9] clause F.3				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
location-info				
Request				
RequestID	"1"	The RequestID that the MCPTT Client will reference in the Report		

5.5.3.5 PIDF

Table 5.5.3.5-1: PIDF

Derivation Path: TS 24.379 [9] subclause 9.3.1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
presence entity	px_MCPTT_Client_A_ID			
tuple id	px_MCPTT_Client_A_ID			
status				
affiliation				
group	px_MCPTT_Group_A_ID			
client	not present			
status				
affiliating				
affiliated	not present			
deaffiliating	not present			
expires	not present			
p-id	any allowed value or same value as sent in SIP PUBLISH	set to an identifier of a SIP PUBLISH request		

5.5.3.6 SIMPLE-FILTER

Table 5.5.3.6-1: SIMPLE-FILTER

Derivation Path: TS 24.379 [9] subclause 9.3.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
filter-set	px_MCPTT_Client_A_ID		RFC 4661 [48]	
nc-bindings	px_MCPTT_Client_A_ID		RFC 4661 [48]	
ns-binding urn	"urn:ietf:params:xml:ns:pidf"		RFC 4661 [48]	
ns-binding urn	"urn:3gpp:ns:mcpttPresInfo:1.0"	TS 24.379 [9] subclause 9.3.2.2 requires two separate ns-binding elements	RFC 4661 [48]	
filter id	"123"	The value of the 'id' attribute has to be unique within the <filter-set> element. Does not contain the 'uri' element. Does not contain the 'domain' element.	RFC 4661 [48]	
what			RFC 4661 [48]	
include	//presence/tuple[@id= px_MCPTT_Client_A_ID]	contains the value, according to IETF RFC 4661 [48], set to concatenation of the '//presence/tuple[@id="' string, the MCPTT client ID, and the '"]' string	RFC 4661 [48]	

5.5.3.7 MCPTT-AFFILIATION-COMMAND

Table 5.5.3.7-1: MCPTT-AFFILIATION-COMMAND

Derivation Path: TS 24.379 [9] clause F.4				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
command-list				
affiliate				
de-affiliate	not present			
group	px_MCPTT_Group_A_ID	MCPTT group name		

5.5.4 Default HTTP message and other information elements

5.5.4.1 General

The HTTP Messages are specified in RFC 2616 [26]. Wherever another reference apply to their content it is explicitly indicated.

The following conditions apply throughout subclause 5.5:

Table 5.5.4-1: Conditions

Condition	Explanation

AUTH	Message/IE sent only as part of a MCPTT UE authentication
USERAUTH	Message/IE sent only as part of a MCPTT UE user authentication
UECONFIG	Message/IE sent only as part of a MCPTT UE configuration
UEUSERPROF	Message/IE sent only as part of a MCPTT UE User profile configuration
UESERVCONFIG	Message/IE sent only as part of a MCPTT UE service configuration
GROUPCONFIG	Message/IE sent only as part of a MCPTT group configuration
TOKEN	Message/IE sent only as part of a MCPTT token exchange
KMSINIT	Message/IE sent only as part of a MCPTT KMS initialisation
KMSKEY	Message/IE sent only as part of a MCPTT KMS key exchange

5.5.4.2 GET

Table 5.5.4.2-1: HTTP GET

Derivation Path: RFC 2616 [26]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-Line				
Method	"GET"			
Request-URI				
uri	px_MCPTT_IdM_Server_URI		TS 33.179 [15]	AUTH
	px_MCPTT_XCAP_UE_Config_URI	points to UE Configuration document	TS 24.484 [14]	UECONFIG
	px_MCPTT_XCAP_User_Profile_URI	points to UE User Profile document	TS 24.484 [14]	UEUSERPROF
	px_MCPTT_XCAP_Service_Config_URI	points to UE Service Configuration document	TS 24.484 [14]	UESERVCONFIG
	px_MCPTT_XCAP_Group_Config_URI	points to group configuration document	TS 24.481 [11]	GROUPCONFIG
query	As described in Table 5.5.4.10.1-1		TS 33.179 [15]	AUTH
HTTP-Version	"HTTP/1.1"			
General header				
Cache-Control	"no-cache"			
Content-Type	"application/x-www-form-urlencoded"			AUTH
Content-Type	"application/x-www-form-urlencoded"			UECONFIG UEUSERPROF UESERVCONFIG GROUPCONFIG
Message-body				
access-token	As described in the field 'access-token' in Table 5.5.4.10.4-1			

5.5.4.3 POST

Table 5.5.4.3-1: HTTP POST

Derivation Path: RFC 2616 [26]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
Method	"POST"			
Request-URI				
uri	px_MCPTT_IdM_Server_URI		TS 33.179 [15]	
query	As described in Table 5.5.4.10.1-1			AUTH
HTTP-Version	"HTTP/1.1"			
General header				
Cache-Control	"no-cache"			
Request Header Fields				USERAUTH
Authorization	px_MCPTT_User_A_username:px_MCPTT_User_A_password	Base64 encoded username:password	RFC 2617 [72]	
Content-Type	"application/x-www-form-urlencoded"			AUTH
Content-Type	"application/x-www-form-urlencoded"		TS 33.179 [15]	TOKEN
Message-body				
Token request	As described in Table 5.5.4.10.3-1			
Content-Type	application/x-www-form-urlencoded		TS 33.179 [15]	KMSINIT
Message-body				
KMS Initialize	As described in Table 5.5.4.10.5-1			
Content-Type	application/x-www-form-urlencoded		TS 33.179 [15]	KMSKEY
Message-body				
KMS KeyProvision	As described in Table 5.5.4.10.7-1			

5.5.4.4 PUT

Table 5.5.4.4-1: HTTP PUT

Derivation Path: RFC 2616 [26]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-line				
Method	"PUT"			
Request-URI	px_MCPTT_GroupConfigDoc_URI	Points to the group configuration document	TS 24.481 [11]	GROUPCONFIG
Content-Type	application/vnd.oma.poc.groups+xml			
Message-body				
group				
xmlns:rl	"urn:ietf:params:xml:ns:resource-lists"	resource-lists xml namespace identifier	TS 24.481 [11]	
xmlns:cp	"urn:ietf:params:xml:ns:common-policy"	common-policy xml namespace identifier	TS 24.481 [11]	
xmlns:ocp	"urn:oma:xml:xdm:common-policy"	common-policy xml namespace identifier	TS 24.481 [11]	
xmlns:oxe	"urn:oma:xml:xdm:extensions"	extensions xml namespace identifier	TS 24.481 [11]	
xmlns:rmcpttgi	"urn:3gpp:ns:mcpttGroupInfo:1.0"	MCPTT group info namespace identifier	TS 24.481 [11]	
list-service				
uri	px_MCPTT_Group_B_ID	uri of the MCPTT group	TS 24.481 [11]	
display-name	px_MCPTT_Group_B_name	group display name	TS 24.481 [11]	
list				
entry				
uri	px_MCPTT_Client_A_ID	User ID allowed to participate in this group	TS 24.481 [11]	
display-name	px_MCPTT_User_A_Profile_Name	User display name	TS 24.481 [11]	
user-priority	1	User priority	TS 24.481 [11]	
entry				
uri	px_MCPTT_Client_B_ID	User ID allowed to participate in this group	TS 24.481 [11]	
display-name	px_MCPTT_User_B_Profile_Name	User display name	TS 24.481 [11]	
user-priority	2	User priority	TS 24.481 [11]	
entry				
uri	px_MCPTT_Client_C_ID	User ID allowed to participate in this group	TS 24.481 [11]	
display-name	px_MCPTT_User_C_Profile_Name	User display name	TS 24.481 [11]	
user-priority	3	User priority	TS 24.481 [11]	
invite-members	"true"	Allow users to invite members to this group	TS 24.481 [11]	
max-participant-count	"3"	Maximum number of users in the group	TS 24.481 [11]	
ruleset				
rule id	"a7c"		TS 24.481 [11]	
actions				
allow-initiate-conf	"true"	All conference calls	TS 24.481 [11]	
join-handling	"true"	Allow group join	TS 24.481 [11]	
emergency-call	"true"	Allow emergency call	TS 24.481 [11]	
imminent-peril-call	"true"	Allow imminent peril call	TS 24.481 [11]	
emergency-alert	"true"	All emergency alert	TS 24.481 [11]	
supported-services				
service-enabler	"urn:urn-7:3gpp-service.ims.icsi.mcptt"		TS 24.481 [11]	
group-priority	"5"	New group priority	TS 24.481 [11]	

5.5.4.5 DELETE

Table 5.5.4.5-1: HTTP DELETE

Derivation Path: RFC 2616 [26]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Request-line				
Method	"DELETE"			
Request-URI	px_MCPTT_GroupConfigDoc_URI	Points to the group configuration document	TS 24.481 [11]	GROUPCONFIG
Content-Type	application/vnd.3gpp.GMOP+xml; charset="utf-8			
Message-body				
gmop:document				
xmlns	"urn:oma:xml:poc:list-service"	list-service xml namespace identifier	TS 24.481 [11]	
xmlns:rl	"urn:ietf:params:xml:ns:resource-lists"	resource-lists xml namespace identifier	TS 24.481 [11]	
xmlns:cp	"urn:ietf:params:xml:ns:common-policy"	common-policy xml namespace identifier	TS 24.481 [11]	
xmlns:ocp	"urn:oma:xml:xdm:common-policy"	common-policy xml namespace identifier	TS 24.481 [11]	
xmlns:oxe	"urn:oma:xml:xdm:extensions"	extensions xml namespace identifier	TS 24.481 [11]	
xmlns:rmcpttgi	"urn:3gpp:ns:mcpttGroupInfo:1.0"	MCPTT group info namespace identifier	TS 24.481 [11]	
xmlns:gmop	"urn:3gpp:ns:mcpttGMOP:1.0"			
gmop:request				
group				
list-service				
uri	"sip:mcptt-group-T@mcptt-op.gov"	Group identifier	TS 24.481 [11]	

5.5.4.6 HTTP 200 (OK)

Table 5.5.4.10-1: HTTP 200 (OK)

Derivation Path: RFC 2616 [26]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
HTTP-Version	"HTTP/1.1"			
Status-Code	"200"			
Reason-Phrase	"OK"			
General header				
Cache-Control	"no-store"			
Pragma	"no-cache"			
Content-Type	"application/json;charset=UTF-8"		TS 33.179 [15]	TOKEN
Message-body				
Token response	As described in Table 5.5.4.10.4-1			
Content-Type	application/x-www-form-urlencoded		TS 33.179 [15]	KMSINIT
Message-body				
KMS Certificate	As described in Table 5.5.4.10.6-1			
Content-Type	application/x-www-form-urlencoded		TS 33.179 [15]	KMSKEY
Message-body				
KMS Key Set	As described in Table 5.5.4.10.8-1			
Content-Type	application/resource-lists+xml		TS 24.484 [14]	UECONFIG
Message-body				
mcptt-UE-configuration	As described in Table 5.5.8.2-1	UE Configuration document returned		
Content-Type	application/resource-lists+xml		TS 24.484 [14]	UEUSERPROF
Message-body				
mcptt-user-profile	As described in Table 5.5.8.3-1	UE User Profile document returned		
Content-Type	application/resource-lists+xml		TS 24.484 [14]	UESERVCONFIG
Message-body				
service-configuration-info	As described in Table 5.5.8.4-1	UE Service Configuration document returned		
Content-Type	application/resource-lists+xml		TS 24.481 [11]	GROUPCONFIG
Message-body				
ue-group-configuration	As described in Table 5.5.7.1-1	Group Configuration document returned		

5.5.4.7 HTTP 201 (Created)

Table 5.5.4.7-1: HTTP 201 (Created)

Derivation Path: RFC 2616 [26]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
HTTP-Version	"HTTP/1.1"			
Status-Code	"20"			
Reason-Phrase	"Created"			
General header				
Cache-Control	"no-store"			
Pragma	"no-cache"			
Content-Type	application/resource-lists+xml		TS 24.483 [13]	GROUPCONFIG
Message-body				
ue-group-configuration	As described in Table 5.5.7.1-1	Group Configuration document returned		

5.5.4.8 HTTP 302 (Found)

Table 5.5.4.8-1: HTTP 302 (Found)

Derivation Path: RFC 2616 [26]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
HTTP-Version	"HTTP/1.1"			
Status-Code	"302"			
Reason-Phrase	"Found"			
Location				AUTH
Location-URI				
uri	px_MCPTT_Client_A_ID	Identifier of the MCPTT client making the API request	TS 33.179 [15]	
query	As described in Table 5.5.4.10.2-1			
Content-Type	"application/x-www-form-urlencoded"		TS 33.179 [15]	AUTH

5.5.4.9 HTTP 409 (Conflict)

Table 5.5.4.9-1: HTTP 409 (Conflict)

Derivation Path: RFC 2616 [26]				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Status-Line				
HTTP-Version	"HTTP/1.1"			
Status-Code	"409"			
Reason-Phrase	"URI constraint violated"	Conflict reason	TS 24.484 [14]	

5.5.4.10 HTTP Message Bodies

5.5.4.10.1 Authentication Request

Table 5.5.4.10.1-1: Authentication Request

Derivation Path: TS 33.179 [15], subclause B.3.1.1				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
response-type	"code"	For native MCPTT clients the value shall be set to "code"	OpenID Connect 1.0 [25]	
client-id	px_MCPTT_Client_A_ID	Identifier of the MCPTT client making the API request	OpenID Connect 1.0 [25]	
scope	″3gpp:mcptt:ptt_server″ ″3gpp:mcptt:key_management_server″ ″3gpp:mcptt:config_management_server″ ″3gpp:mcptt:group_management_server″	Scope values are expressed as a list of space-delimited, case-sensitive strings which indicate which MCPTT resource servers the client is requesting access to	TS 33.179 [15]	
redirect-uri	px_MCPTT_User_A_Organization	The URI of the MCPTT client to which the IdM server will redirect the MCPTT client's user agent in order to return the authorization code	OpenID Connect 1.0 [25]	
state	"abc123"	An opaque value used by the MCPTT client to maintain state between the authorization request and authorization response	OpenID Connect 1.0 [25]	
acr-values	"3gpp:acr:password"	Space-separated string that specifies the acr values that the IdM server is being requested to use for processing this authorization request	TS 33.179 [15]	
code-challenge	"123456789"	base64url-encoded SHA-256 challenge	TS 33.179 [15]	
code-challenge-method	"S256"	The hash method used to transform the code verifier to produce the code challenge	TS 33.179 [15]	

5.5.4.10.2 Authentication Response

Table 5.5.4.10.2-1: Authentication Response

Derivation Path: TS 33.179 [15], subclause B.3.1.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
code	"SplxlOBeZQQYbYS6WxSbIA"	The authorization code generated by the authorization endpoint and returned to the MCPTT client via the authorization response	TS 33.179 [15]	
state	"abc123"	The value shall match the exact value used in the authorization request	TS 33.179 [15]	

5.5.4.10.3 Token Request

Table 5.5.4.10.3-1: Token Request

Derivation Path: TS 33.179 [15], subclause B.3.1.3				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
grant-type	"authorization_code"		RFC 2616 [26]	
code	"SplxlOBeZQQYbYS6WxSbIA"	The authorization code generated by the authorization endpoint and returned to the MCPTT client via the authorization response	TS 33.179 [15]	
mcptt-client-id	px_MCPTT_Client_A_ID	Identifier of the MCPTT client making the API request	TS 33.179 [15]	
redirect-uri	px_MCPTT_User_A_Organization	The URI of the MCPTT client to which the IdM server will redirect the MCPTT client's user agent	TS 33.179 [15]	
code-verifier	"123456789"	A cryptographically random string that is used to correlate the authorization request to the token request	TS 33.179 [15]	

5.5.4.10.4 Token Response

Table 5.5.4.10.4-1: Token Response

Derivation Path: TS 33.179 [15], subclause B.3.1.4				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
access-token	"eyJhbGciOiJSUzI1NiJ9.eyJtY3B0dF9pZCI6ImFsaWNlQG9yZy5jb20iLCJleHAiOjE0NTM1MDYxMjEsInNjb3BlIjpbIm9wZW5pZCIsIjNncHA6bWNwdHQ6cHR0X3NlcnZlciJdLCJjbGllbnRfaWQiOiJtY3B0dF9jbGllbnQifQ.XYIqai4YKSZCKRNMLipGC_5nV4BE79IJpvjexWjIqqcqiEx6AmHHIRo0mhcxeCESrXei9krom9e8Goxr_hgF3szvgbwl8JRbFuv97XgepDLjEq4jL3Cbu41Q9b0WdXAdFmeEbiB8wo_xggiGwv6IDR1b3TgAAsdjkRxSK4ctIKPaOJSRmM7MKMcKhIug3BEkSC9-aXBTSIv5fAGN-ShDbPvHycBpjzKWXBvMIR5PaCg-9fwjELXZXdRwz8C6JbRM8aqzhdt4CVhQ3-Arip-S9CKd0tu-qhHfF2rvJDRlg8ZBiihdPH8mJs-qpTFep_1-kON3mL0_g54xVmIMwN0XQA"	The access token. The access token is opaque to the MCPTT client	RFC 6749 [77]	
refresh-token	"Y7NSzUJuS0Jp7G4SKpBKSOJVHIZxFbxqsqCIZhOEk9"	The refresh token that can be used to refresh the access token and avoid having to prompt the user for authentication again	RFC 6749 [77]	
id-token	"eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiYXVkIjoibWNwdHRfY2xpZW50IiwiaXNzIjoiSWRNUy5zZXJ2ZXIuY29tOjkwMzEiLCJpYXQiOjE0NTM0OTgxNTgsImV4cCI6MTQ1MzQ5ODQ1OCwibWNwdHRfaWQiOiJhbGljZUBvcmcuY29tIn0.Dpn7AhIMaqMEgg12NYUUfJGSFJMPG8M2li9FLtPotDlHvwU2emBws8z5JLw81SXQnoLqZ8ZF8tIhZ1W7uuMbufF4Wsr7PAadZixz3CnV2wxFV9qR_VA1-0ccDTPukUsRHsic0SgZ3aIbcYKd6VsehFe_GDwfqysYzD7yPwCfPZo"	The MCPTT client may validate the user with the ID token and configure itself for the user	RFC 6749 [77]	
token-type	"Bearer"	The token type for access	RFC 6749 [77]	
expires-in	"7199"	Token expiry time	RFC 6749 [77]	

5.5.4.10.5 KMS Initialize

Table 5.5.4.10.5-1: KMS Initialize

Derivation Path: TS 33.179 [15], subclause D.3.1.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
id-token	"eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiYXVkIjoibWNwdHRfY2xpZW50IiwiaXNzIjoiSWRNUy5zZXJ2ZXIuY29tOjkwMzEiLCJpYXQiOjE0NTM0OTgxNTgsImV4cCI6MTQ1MzQ5ODQ1OCwibWNwdHRfaWQiOiJhbGljZUBvcmcuY29tIn0.Dpn7AhIMaqMEgg12NYUUfJGSFJMPG8M2li9FLtPotDlHvwU2emBws8z5JLw81SXQnoLqZ8ZF8tIhZ1W7uuMbufF4Wsr7PAadZixz3CnV2wxFV9qR_VA1-0ccDTPukUsRHsic0SgZ3aIbcYKd6VsehFe_GDwfqysYzD7yPwCfPZo"	The MCPTT client may validate the user with the ID token and configure itself for the user	RFC 6749 [77]	
access-token	"eyJhbGciOiJSUzI1NiJ9.eyJtY3B0dF9pZCI6ImFsaWNlQG9yZy5jb20iLCJleHAiOjE0NTM1MDYxMjEsInNjb3BlIjpbIm9wZW5pZCIsIjNncHA6bWNwdHQ6cHR0X3NlcnZlciJdLCJjbGllbnRfaWQiOiJtY3B0dF9jbGllbnQifQ.XYIqai4YKSZCKRNMLipGC_5nV4BE79IJpvjexWjIqqcqiEx6AmHHIRo0mhcxeCESrXei9krom9e8Goxr_hgF3szvgbwl8JRbFuv97XgepDLjEq4jL3Cbu41Q9b0WdXAdFmeEbiB8wo_xggiGwv6IDR1b3TgAAsdjkRxSK4ctIKPaOJSRmM7MKMcKhIug3BEkSC9-aXBTSIv5fAGN-ShDbPvHycBpjzKWXBvMIR5PaCg-9fwjELXZXdRwz8C6JbRM8aqzhdt4CVhQ3-Arip-S9CKd0tu-qhHfF2rvJDRlg8ZBiihdPH8mJs-qpTFep_1-kON3mL0_g54xVmlMwN0XQA"	The access token. The access token is opaque to the MCPTT client	RFC 6749 [77]	

5.5.4.10.6 KMS Certificate

Table 5.5.4.10.6-1: KMS Certificate

Derivation Path: TS 33.179 [15], subclause D.3.1.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Version	"1.1.0"	The version number of the certificate type		
Role	"Root"	This shall indicate whether the certificate is a "Root" or "External" certificate		
CertUri	px_MCPTT_CertUri	The URI of the Certificate (this object)		
KmsUri	px_MCPTT_KmsUri	The URI of the KMS which issued the Certificate		
Issuer	No value	(Optional) String describing the issuing entity		
ValidFrom	No value	(Optional) Date from which the Certificate may be used		
ValidTo	No value	(Optional) Date at which the Certificate expires		
Revoked	false	(Optional) A Boolean value defining whether a Certificate has been revoked		
UserIDFormat	"2"	Shall contain the value '2'		
UserKeyPeriod	"2592000"	The number of seconds that each user key issued by this KMS should be used		
UserKeyOffset	"0"	The offset in seconds from 0h on 1st Jan 1900 that the segmentation of key periods starts		
PubEncKey	"029A2F"	The SAKKE Public Key, "Z_T". This is an OCTET STRING encoding of an elliptic curve point		
PubAuthKey	"029A2F"	The ECCSI Public Key, "KPAK". This is an OCTET STRING encoding of an elliptic curve point		
ParameterSet	No value	(Optional) The choice of parameter set used for SAKKE and ECCSI		
KmsDomainList	No value	(Optional) List of domains associated with the certificate		

5.5.4.10.7 KMS KeyProvision

Table 5.5.4.10.7-1: KMS KeyProvision

Derivation Path: TS 33.179 [15], subclause D.3.1.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
id-token	"eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiYXVkIjoibWNwdHRfY2xpZW50IiwiaXNzIjoiSWRNUy5zZXJ2ZXIuY29tOjkwMzEiLCJpYXQiOjE0NTM0OTgxNTgsImV4cCI6MTQ1MzQ5ODQ1OCwibWNwdHRfaWQiOiJhbGljZUBvcmcuY29tIn0.Dpn7AhIMaqMEgg12NYUUfJGSFJMPG8M2li9FLtPotDlHvwU2emBws8z5JLw81SXQnoLqZ8F8tIhZ1W7uuMbufF4Wsr7PAadZixz3CnV2wxFV9qR_VA1-0ccDTPukUsRHsic0SgZ3aIbcYKd6VsehFe_GDwfqysYzD7yPwCfPZo"	The MCPTT client may validate the user with the ID token and configure itself for the user	RFC 6749 [77]	
access-token	"eyJhbGciOiJSUzI1NiJ9.eyJtY3B0dF9pZCI6ImFsaWNlQG9yZy5jb20iLCJleHAiOjE0NTM1MDYxMjEsInNjb3BlIjpbIm9wZW5pZCIsIjNncHA6bWNwdHQ6cHR0X3NlcnZlciJdLCJjbGllbnRfaWQiOiJtY3B0dF9jbGllbnQifQ.XYIqai4YKSZCKRNMLipGC_5nV4BE79IJpvjexWjIqqcqiEx6AmHHIRo0mhcxeCESrXei9krom9e8Goxr_hgF3szvgbwl8JRbFuv97XgepDLjEq4jL3Cbu41Q9b0WdXAdFmeEbiB8wo_xggiGwv6IDR1b3TgAAsdjkRxSK4ctIKPaOJSRmM7MKMcKhIug3BEkSC9-aXBTSIv5fAGN-ShDbPvHycBpjzKWXBvMIR5PaCg-9fwjELXZXdRwz8C6JbRM8aqzhdt4CVhQ3-Arip-S9CKd0tu-qhHfF2rvJDRlg8ZBiihdPH8mJs-qpTFep_1-kON3mL0_g54xVmlMwN0XQA"	The access token. The access token is opaque to the MCPTT client	RFC 6749 [77]	

5.5.4.10.8 KMS Key Set

Table 5.5.4.10.8-1: KMS Key Set

Derivation Path: TS 33.179 [15], subclause D.3.2.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
KmsResponse				
KmsUri	px_MCPTT_KmsUri	The URI of the KMS which issued the key set		
UserUri	px_MCPTT_Client_A_ID	URI of the user for which the key set is issued		
Time	Any Value	Time stamp of KMS message		
KmsId	px_MCPTT_KmsId	The ID of the KMS that issues the key set		
ClientReqUrl	px_MCPTT_KmsClientUrl	URL of the client making the key request		
KmsMessage				
KmsKeyProvVersion	"1.1.0"	The version number of the key provision XML		
KmsKeySetVersion	"1.1.0"	The version number of the key set XML		
KmsUri	px_MCPTT_KmsUri	The URI of the KMS which issued the key set		
CertUri	No value	(Optional) The URI of the Certificate which may be used to validate the key set		
Issuer	No value	(Optional) String describing the issuing entity		
UserUri	px_MCPTT_Client_A_ID	URI of the user for which the key set is issued		
UserID	"123456789ABCDEF"	UID corresponding to the key set		
ValidFrom	No value	(Optional) Date and time from which the key set may be used		
ValidTo	No value	(Optional) Date and time at which the key set expires		
KeyPeriodNo	"1514"	Current Key Period No. since 1 January 1900		
Revoked	"false"	(Optional) A Boolean value defining whether the key set has been revoked		
UserDecryptKey		The SAKKE "Receiver Secret Key". This is an OCTET STRING encoding of an elliptic curve point		
EncryptionAlgorithm	"AES256"	Encryption algorithm to use		
KeyInfo:key-name	px_MCPTT_UserDecryptKey_name	Key name		
CipherData:value	"1212ADDF"	Key value		
UserSigningKeySSK		The ECCSI private Key, "SSK". This is an OCTET STRING encoding of an integer		
EncryptionAlgorithm	"AES256"	Encryption algorithm to use		
KeyInfo:key-name	px_MCPTT_UserSigningKeySSK_name	Key name		
CipherData:value	"1212ADDF"	Key value		

Derivation Path: TS 33.179 [15], subclause D.3.2.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
KmsResponse				
UserPubTokenPVT		The ECCSI public validation token, "PVT". This is an OCTET STRING encoding of an elliptic curve point		
EncryptionAlgorithm	"AES256"	Encryption algorithm to use		
KeyInfo:key-name	px_MCPTT_UserPubTokenPVT_name	Key name		
CipherData:value	"1212ADDF"	Key value		
Signature:xmlns				
SignedInfo				
CanonicalizationAlgorithm	"xml-c14n"	XML Signature processing		
SignatureAlgorithm	"SHA-256"	Hashing algorithm to use		
DigestAlgorithm	"SHA-256"	Hashing algorithm to use		
DigestValue	Any Value	Determined by hash value		
SignatureValue	Any Value	Determined by hash value		
KeyInfo:key-name	px_MCPTT_SigningKey_name	Key name used to sign KMS messages		

5.5.5 Default MCPTT call control Off-network messages and other information elements

5.5.5.1 GROUP CALL PROBE

Table 5.5.5.1-1: GROUP CALL PROBE

Derivation Path: TS 24.379 [9] Table 15.1.2.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		

5.5.5.2 GROUP CALL ANNOUNCEMENT

5.5.5.2.1 GROUP CALL ANNOUNCEMENT from the UE

Table 5.5.5.2.1-1: GROUP CALL ANNOUNCEMENT from the UE

Derivation Path: TS 24.379 [9] Table 15.1.3.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65535) generated at the beginning of a call establishment		
Call type	"00000001"	Basic Group Call	
Refresh interval	10000	The Refresh interval contains a number denoting the minimum time interval (milliseconds) between two successive periodic announcements. NOTE: In release 13.7 of TS 24.379 [9], the refresh interval of the call is fixed to 10 seconds.	
Call start time	The Call start time value is an unsigned integer containing UTC time of the time when a call was started, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).		
Last call type change time	The Last call type change time value is an unsigned integer containing UTC time of the time when a call priority was changed, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).		
MCPTT group ID	px_MCPTT_Group_A_ID		
SDP	As described in Table 5.5.3.1.3-1		
Originating MCPTT user ID	px_MCPTT_User_A_ID	pre-set MCPTT user ID	
Last user to change call type	The ID of the last user to change contents		
Confirm mode indication	Present		
Probe response	Not Present		

5.5.5.2.2 GROUP CALL ANNOUNCEMENT from the SS

Table 5.5.5.2.2-1: GROUP CALL ANNOUNCEMENT from the SS

Derivation Path: TS 24.379 [9] Table 15.1.3.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65535) generated at the beginning of a call establishment		
Call type	"00000001"	Basic Group Call	
Refresh interval	10000	The Refresh interval contains a number denoting the minimum time interval (milliseconds) between two successive periodic announcements. NOTE: In release 13.7 of TS 24.379 [9], the refresh interval of the call is fixed to 10 seconds.	
Call start time	The Call start time value is an unsigned integer containing UTC time of the time when a call was started, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).		
Last call type change time	The Last call type change time value is an unsigned integer containing UTC time of the time when a call priority was changed, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).		
MCPTT group ID	px_MCPTT_Group_A_ID		
SDP	As described in Table 5.5.3.1.4-1		
Originating MCPTT user ID	px_MCPTT_User_B_ID	pre-set MCPTT user ID	
Last user to change call type	The ID of the last user to change contents		
Confirm mode indication	Present		
Probe response	Not Present		

5.5.5.3 GROUP CALL ACCEPT

5.5.5.3.1 GROUP CALL ACCEPT from the UE

Table 5.5.5.3.1-1: GROUP CALL ACCEPT from the UE

Derivation Path: TS 24.379 [9] Table 15.1.4.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Call type	"00000001"	Basic Group Call	
MCPTT group ID	px_MCPTT_Group_A_ID		
Sending MCPTT user ID	px_MCPTT_User_A_ID		

5.5.5.3.2 GROUP CALL ACCEPT from the SS

Table 5.5.5.3.2-1: GROUP CALL ACCEPT from the SS

Derivation Path: TS 24.379 [9] Table 15.1.4.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Call type	"00000001"	Basic Group Call	
MCPTT group ID	px_MCPTT_Group_A_ID		
Sending MCPTT user ID	px_MCPTT_User_B_ID		

5.5.5.4 GROUP CALL EMERGENCY END

5.5.5.4.1 GROUP CALL EMERGENCY END from the UE

Table 5.5.5.4.1-1: GROUP CALL EMERGENCY END from the UE

Derivation Path: TS 24.379 [9] Table 15.1.15.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Last call type change time	The Last call type change time value is an unsigned integer containing UTC time of the time when a call priority was changed, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).		
Last user to change call type	The ID of the last user to change contents		
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_A_ID		

5.5.5.4.2 GROUP CALL EMERGENCY END from the SS

Table 5.5.5.4.2-1: GROUP CALL EMERGENCY END from the SS

Derivation Path: TS 24.379 [9] Table 15.1.15.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Last call type change time	The Last call type change time value is an unsigned integer containing UTC time of the time when a call priority was changed, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).		
Last user to change call type	The ID of the last user to change contents		
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_B_ID		

5.5.5.5 GROUP CALL IMMINENT PERIL END

5.5.5.5.1 GROUP CALL IMMINENT PERIL END from the UE

Table 5.5.5.5.1-1: GROUP CALL IMMINENT PERIL END from the UE

Derivation Path: TS 24.379 [9] Table 15.1.14.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Last call type change time	The Last call type change time value is an unsigned integer containing UTC time of the time when a call priority was changed, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).		
Last user to change call type	The ID of the last user to change contents		
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_A_ID		

5.5.5.5.2 GROUP CALL IMMINENT PERIL END from the SS

Table 5.5.5.5.2-1: GROUP CALL IMMINENT PERIL END from the SS

Derivation Path: TS 24.379 [9] Table 15.1.14.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Last call type change time	The Last call type change time value is an unsigned integer containing UTC time of the time when a call priority was changed, in seconds since midnight UTC of January 1, 1970 (not counting leap seconds).		
Last user to change call type	The ID of the last user to change contents		
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_B_ID		

5.5.5.6 GROUP CALL BROADCAST

5.5.5.6.1 GROUP CALL BROADCAST from the UE

Table 5.5.5.6.1-1: GROUP CALL BROADCAST from the UE

Derivation Path: TS 24.379 [9] Table 15.1.20.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Call type	"00000010"	Broadcast Group Call	
Originating MCPTT user ID	px_MCPTT_User_A_ID		
MCPTT group ID	px_MCPTT_Group_A_ID		
SDP	As described in Table 5.5.3.1.3-1		

5.5.5.6.2 GROUP CALL BROADCAST from the SS

Table 5.5.5.6.2-1: GROUP CALL BROADCAST from the SS

Derivation Path: TS 24.379 [9] Table 15.1.20.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Call type	"00000010"	Broadcast Group Call	
Originating MCPTT user ID	px_MCPTT_User_B_ID		
MCPTT group ID	px_MCPTT_Group_A_ID		
SDP	As described in Table 5.5.3.1.4-1		

5.5.5.7 GROUP CALL BROADCAST END

5.5.5.7.1 GROUP CALL BROADCAST END from the UE

Table 5.5.5.7.1-1: GROUP CALL BROADCAST END from the UE

Derivation Path: TS 24.379 [9] Table 15.1.21.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
MCPTT group ID	px_MCPTT_Group_A_ID		
SDP	As described in Table 5.5.3.1.3-1		

5.5.5.7.2 GROUP CALL BROADCAST END from the SS

Table 5.5.5.7.2-1: GROUP CALL BROADCAST END from the SS

Derivation Path: TS 24.379 [9] Table 15.1.21.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
MCPTT group ID	px_MCPTT_Group_A_ID		
SDP	As described in Table 5.5.3.1.4-1		

5.5.5.8 PRIVATE CALL SETUP REQUEST

5.5.5.8.1 PRIVATE CALL SETUP REQUEST from the UE

Table 5.5.5.8.1-1: PRIVATE CALL SETUP REQUEST from the UE

Derivation Path: 24.379 [9], Table 15.1.5.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Commencement mode	"00000000"	Automatic Commencement Mode	
Call type	"00000101"	Private Call	
MCPTT user ID of the caller	px_MCPTT_User_A_ID		
MCPTT user ID of the callee	px_MCPTT_User_B_ID		
SDP offer	As described in Table 5.5.3.1.3-1		
User location	Not Present		

5.5.5.8.2 PRIVATE CALL SETUP REQUEST from the SS

Table 5.5.5.8.2-1: PRIVATE CALL SETUP REQUEST from the SS

Derivation Path: 24.379 [9], Table 15.1.5.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
Commencement mode	"00000000"	Automatic Commencement Mode	
Call type	"00000101"	Private Call	
MCPTT user ID of the caller	px_MCPTT_User_B_ID		
MCPTT user ID of the callee	px_MCPTT_User_A_ID		
SDP offer	As described in Table 5.5.3.1.4-1		
User location	Not Present		

5.5.5.9 PRIVATE CALL RINGING

Table 5.5.5.9-1: PRIVATE CALL RINGING

Derivation Path: 24.379 [9], Table 15.1.6.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the caller	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the callee	Same as the one in PRIVATE CALL SETUP REQUEST		

5.5.5.10 PRIVATE CALL ACCEPT

Table 5.5.5.10-1: PRIVATE CALL ACCEPT

Derivation Path: 24.379 [9], Table 15.1.7.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the caller	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the callee	Same as the one in PRIVATE CALL SETUP REQUEST		
SDP answer	Same as the one in PRIVATE CALL SETUP REQUEST		

5.5.5.11 PRIVATE CALL REJECT

5.5.5.11.1 PRIVATE CALL REJECT from the UE

Table 5.5.5.11.1-1: PRIVATE CALL REJECT from the UE

Derivation Path: 24.379 [9], Table 15.1.8.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL SETUP REQUEST		
Reason	Any allowed value		
MCPTT user ID of the caller	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the callee	Same as the one in PRIVATE CALL SETUP REQUEST		
SDP answer	As described in Table 5.5.3.1.3-1		

5.5.5.11.2 PRIVATE CALL REJECT from the SS

Table 5.5.5.11.2-1: PRIVATE CALL REJECT from the SS

Derivation Path: 24.379 [9], Table 15.1.8.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL SETUP REQUEST		
Reason	"00000000"	Reason = REJECT	
MCPTT user ID of the caller	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the callee	Same as the one in PRIVATE CALL SETUP REQUEST		
SDP answer	As described in Table 5.5.3.1.4-1		

5.5.5.12 PRIVATE CALL RELEASE

Table 5.5.5.12-1: PRIVATE CALL RELEASE

Derivation Path: 24.379 [9], Table 15.1.9.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the caller	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the callee	Same as the one in PRIVATE CALL SETUP REQUEST		

5.5.5.13 PRIVATE CALL RELEASE ACK

Table 5.5.5.13-1: PRIVATE CALL RELEASE ACK

Derivation Path: 24.379 [9], Table 15.1.10.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the caller	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the callee	Same as the one in PRIVATE CALL SETUP REQUEST		

5.5.5.14 PRIVATE CALL ACCEPT ACK

Table 5.5.5.14-1: PRIVATE CALL ACCEPT ACK

Derivation Path: 24.379 [9], Table 15.1.11.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the caller	Same as the one in PRIVATE CALL SETUP REQUEST		
MCPTT user ID of the callee	Same as the one in PRIVATE CALL SETUP REQUEST		

5.5.5.15 PRIVATE CALL EMERGENCY CANCEL

5.5.5.15.1 PRIVATE CALL EMERGENCY CANCEL from the UE

Table 5.5.5.15.1-1: PRIVATE CALL EMERGENCY CANCEL from the UE

Derivation Path: 24.379 [9], Table 15.1.12.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
MCPTT user ID of the caller	px_MCPTT_User_A_ID		
MCPTT user ID of the callee	px_MCPTT_User_B_ID		

5.5.5.15.2 PRIVATE CALL EMERGENCY CANCEL from the SS

Table 5.5.5.15.2-1: PRIVATE CALL EMERGENCY CANCEL from the SS

Derivation Path: 24.379 [9], Table 15.1.12.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	a random number uniformly distributed between (0, 65536) generated at the beginning of a call establishment		
MCPTT user ID of the caller	px_MCPTT_User_B_ID		
MCPTT user ID of the callee	px_MCPTT_User_A_ID		

5.5.5.16 PRIVATE CALL EMERGENCY CANCEL ACK

5.5.5.16.1 PRIVATE CALL EMERGENCY CANCEL ACK from the UE

Table 5.5.5.16.1-1: PRIVATE CALL EMERGENCY CANCEL ACK from the UE

Derivation Path: 24.379 [9], Table 15.1.13.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL EMERGENCY CANCEL		
MCPTT user ID of the caller	px_MCPTT_User_A_ID		
MCPTT user ID of the callee	px_MCPTT_User_B_ID		

5.5.5.16.2 PRIVATE CALL EMERGENCY CANCEL ACK from the SS

Table 5.5.5.16.2-1: PRIVATE CALL EMERGENCY CANCEL ACK from the SS

Derivation Path: 24.379 [9], Table 15.1.13.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Call identifier	Same as the one in PRIVATE CALL EMERGENCY CANCEL		
MCPTT user ID of the caller	px_MCPTT_User_B_ID		
MCPTT user ID of the callee	px_MCPTT_User_A_ID		

5.5.5.17 GROUP EMERGENCY ALERT

5.5.5.17.1 GROUP EMERGENCY ALERT from the UE

Table 5.5.5.17.1-1: GROUP EMERGENCY ALERT from the UE

Derivation Path: TS 24.379 [9] Table 15.1.16.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_A_ID		
Organization name	Any allowed value		
User location	Not Present		

5.5.5.17.2 GROUP EMERGENCY ALERT from the SS

Table 5.5.5.17.2-1: GROUP EMERGENCY ALERT from the SS

Derivation Path: TS 24.379 [9] Table 15.1.16.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_B_ID		
Organization name	px_MCPTT_Group_A_Owner_Organization		
User location	Not Present		

5.5.5.18 GROUP EMERGENCY ALERT ACK

5.5.5.18.1 GROUP EMERGENC ALERT ACK from the UE

Table 5.5.5.18.1-1: GROUP EMERGENCY ALERT ACK from the UE

Derivation Path: TS 24.379 [9] Table 15.1.17.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_B_ID		
Sending MCPTT user ID	px_MCPTT_User_A_ID		

5.5.5.18.2 GROUP EMERGENC ALERT ACK from the SS

Table 5.5.5.18.2-1: GROUP EMERGENCY ALERT ACK from the SS

Derivation Path: TS 24.379 [9] Table 15.1.17.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_A_ID		
Sending MCPTT user ID	px_MCPTT_User_B_ID		

5.5.5.19 GROUP EMERGENCY ALERT CANCEL

5.5.5.19.1 GROUP EMERGENCY ALERT CANCEL from the UE

Table 5.5.5.19.1-1: GROUP EMERGENCY ALERT CANCEL from the UE

Derivation Path: TS 24.379 [9] Table 15.1.18.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_A_ID		
Sending MCPTT user ID	px_MCPTT_User_A_ID		

5.5.5.19.2 GROUP EMERGENCY ALERT CANCEL from the SS

Table 5.5.5.19.2-1: GROUP EMERGENCY ALERT CANCEL from the SS

Derivation Path: TS 24.379 [9] Table 15.1.18.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_B_ID		
Sending MCPTT user ID	px_MCPTT_User_B_ID		

5.5.5.20 GROUP EMERGENCY ALERT CANCEL ACK

5.5.5.20.1 GROUP EMERGENCY ALERT CANCEL ACK from the UE

Table 5.5.5.20.1-1: GROUP EMERGENCY ALERT CANCEL ACK from the UE

Derivation Path: TS 24.379 [9] Table 15.1.19.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_B_ID		
Sending MCPTT user ID	px_MCPTT_User_A_ID		

5.5.5.20.2 GROUP EMERGENCY ALERT CANCEL ACK from the SS

Table 5.5.5.20.2-1: GROUP EMERGENCY ALERT CANCEL ACK from the SS

Derivation Path: TS 24.379 [9] Table 15.1.19.1-1			
Information Element	**Value/remark**	**Comment**	**Condition**
MCPTT group ID	px_MCPTT_Group_A_ID		
Originating MCPTT user ID	px_MCPTT_User_A_ID		
Sending MCPTT user ID	px_MCPTT_User_B_ID		

5.5.6 Default MCPTT media plane control messages and other information elements

5.5.6.1 General

The media plane control protocols messages specified in the present document are based on those specified in TS 24.380 [10] which in term are based on the RTCP Application Packets (RTCP: APP), as defined in IETF RFC 3550 [76].

Depending on the TC scenario, the same MCPTT media plane control message can be sent by the SS or by the UE. Throughout the default content specified in below a particular value has been chosen to satisfy one or the other scenario. It is expected that when a message is used in a TC in a particular context then the relevant for the usage in the TC values will be defined in the TC.

The following conditions apply throughout subclause 5.5.6:

Table 5.5.6.1-1: Conditions

Condition	Explanation
ON-NETWORK	Message sent in on-network scenario.
OFF-NETWORK	Message sent in off-network scenario.
PRIVATE-CALL	Message sent as part of a Private call handling.
GROUP-CALL	Message sent as part of a Group call handling.

Considerations in regard to describing specifc values:

- SSRC
  - Synchronization SouRCe (SSRC) values are used in most of the messages specified in subclause 5.5.6. The SSRC value is randomly chosen by the participant in, and globally unique within, an RTP session as specified in IETF RFC 3550 [76]. Because the value chosen by the UE (MCPTT client) cannot be controlled, specifying a "hard coded" value to be used by the SS (MCPTT server) or the SS-UE (MCPTT Client) is prone to triggering a collision by chosing a value which may be the same as the one chosen by the UE. How to resolve SSRC collisions is described in IETF RFC 3550 [76] however, resolving them as part of the MMCPT test case defintions e.g. in TS 36.579-2 [2] is not foreseen and is left to the test implementation.
  - For the purposes of default and specific messages defintion throughout the present specification, as well as, throughout the rest of the MCPTT conformance test specifications e.g. the TS 36.579-2 [2] no explicit SSRC values are defined and instead the folowing notation is used to clarify the messages origin/destination:
    - When there is no dangeour for misunderstanding the notation 'The SSRC of the message sender' and the 'The SSRC of the intended recipient of the message' are used whereas the "sender" and the "recipient" are to be udnerstood in the context of the test i.e. the test entities being involved to exchange messages

- When in doubt, the notations 'UE (MCPTT client) SSRC', SS (MCPTT server) SSRC', 'SS-UE1 (MCPTT Client) SSRC' or 'SS-UE2 (MCPTT Client) SSRC' are used.

5.5.6.2 Floor Request

Table 5.5.6.2-1: Floor Request

Derivation Path: 24.380 [10], Table 8.2.4-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor participant sending the message. Notation in accordance with subclause 5.5.6.1.	
Floor priority	Not present or Any allowed value	If present, a value between ‘0’ and ‘255’ where '0' is the lowest priority If the Floor Priority field is not included in the message the default priority (='0') is used as the Floor Priority value The max floor priority that can be requested in a Floor Request message is negotiated between the MCPTT client and the controlling MCPTT function using the "mc_priority" fmtp parameter e.g. at call setup	
User ID	Not present		ON-NETWORK
User ID			OFF-NETWORK
User ID	px_MCPTT_User_A_ID	The MCPTT User ID of the floor participant requesting the floor.	
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	
Floor Indicator			
Floor Indicator	Any allowed value		

5.5.6.3 Floor Granted

Table 5.5.6.3-1: Floor Granted

Derivation Path: 24.380 [10], Table 8.2.5-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPT		
Duration			
Duration	"00000000 10000000"	128 sec (an arbitrary value)	
SSRC of granted floor participant	The SSRC of the intended recipient of the message	Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
Floor priority	Not present	If the Floor Priority field is not included in the message the default priority (='0') is used as the Floor Priority value	
User ID	Not present		ON-NETWORK
User ID			OFF-NETWORK
User ID	px_MCPTT_User_A_ID	The MCPTT User ID of the floor participant granted the floor.	
Queue Size	Not present		ON-NETWORK
Queue Size	"0"	the number of queued MCPTT clients in the MCPTT call	OFF-NETWORK
SSRC of queued floor participant	Not present		
Queued User ID	Not present		
Queue Info	Not present		
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	
Floor Indicator			
Floor Indicator	Any allowed value		

5.5.6.4 Floor Deny

Table 5.5.6.4-1: Floor Deny

Derivation Path: 24.380 [10], Table 8.2.6-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPT		
Reject Cause			
Reject Cause	"1"	Cause #1 - Another MCPTT client has permission	
Reject Phrase	"Another MCPTT client has permission"	An additional text string explaining the reason for rejecting the floor request.	
User ID	Not present		ON-NETWORK
User ID			OFF-NETWORK
User ID	px_MCPTT_User_A_ID	The MCPTT User ID of the floor participant being denied floor request.	
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	
Floor Indicator			
Floor Indicator	Any allowed value		

5.5.6.5 Floor Release

Table 5.5.6.5-1: Floor Release

Derivation Path: 24.380 [10], Table 8.2.7-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor participant sending the message. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76]	
name	MCPT		
User ID	Not present		ON-NETWORK
User ID			OFF-NETWORK
User ID	px_MCPTT_User_A_ID	The MCPTT User ID of the floor participant releasing the floor.	
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	
Floor Indicator			
Floor Indicator	Any allowed value		

5.5.6.6 Floor Idle

Table 5.5.6.6-1: Floor Idle

Derivation Path: 24.380 [10], Table 8.2.8-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPT		
Message Sequence Number			
Message Sequence Number	The value sent in the previous Floor Idle message, if any, increased with 1	Any value between '0' and '65535' When the '65535' value is reached, the <Message Sequence Number> value starts from '0' again	
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	
Floor Indicator			
Floor Indicator	Any allowed value		

5.5.6.7 Floor Taken

Table 5.5.6.7-1: Floor Taken

Derivation Path: 24.380 [10], Table 8.2.9-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPT		
User ID	Not present		ON-NETWORK
User ID			OFF-NETWORK
User ID	px_MCPTT_User_A_ID	The MCPTT user ID of the floor participant sending the Floor Taken message	
Granted Party's Identity			
Granted Party's Identity	px_MCPTT_User_B_ID	The MCPTT User ID of the floor participant being granted the floor.	
Permission to Request the Floor			
Permission to Request the Floor	"1"	The receiver is permitted to request floor	
Message Sequence Number			
Message Sequence Number	The value sent in the previous Floor Taken message, if any, increased with 1	Any value between '0' and '65535' When the '65535' value is reached, the <Message Sequence Number> value starts from '0' again	
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	
Floor Indicator			
Floor Indicator	Any allowed value		
SSRC of granted floor participant	SS-UE1 (MCPTT Client) SSRC	The SSRC of the granted floor participant.	

5.5.6.8 Floor Revoke

Table 5.5.6.8-1: Floor Revoke

Derivation Path: 24.380 [10], Table 8.2.10.1-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPT		
Reject Cause			
Reject Cause	"4"	Cause#4 - Media Burst pre-empted	
Reject Phrase	"Media Burst pre-empted"	a text string encoded the text string in the SDES item CNAME as specified in IETF RFC 3550 [76], subclause 6.5.1.	
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	
Floor Indicator			
Floor Indicator	Any allowed value		

5.5.6.9 Floor Queue Position Request

Table 5.5.6.9-1: Floor Queue Position Request

Derivation Path: 24.380 [10], Table 8.2.11-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor participant sending the message. Notation in accordance with subclause 5.5.6.1. Codedas specified in IETF RFC 3550 [76]	
name	MCPT		
User ID	Not present		ON-NETWORK
User ID			OFF-NETWORK
User ID	px_MCPTT_User_A_ID	The MCPTT ID of the floor participant requesting the information.	
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	

5.5.6.10 Floor Queue Position Info

Table 5.5.6.10-1: Floor Queue Position Info

Derivation Path: 24.380 [10], Table 8.2.12-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPT		
User ID	Not present		ON-NETWORK
User ID			OFF-NETWORK
User ID	px_MCPTT_User_B_ID	the MCPTT ID of the floor participant sending the Floor Queue Position Info message	
SSRC of queued floor participant	Not present		ON-NETWORK
	The SSRC of the message recepient	The SSRC field carries the SSRC of the queued floor participant	OFF-NETWORK
Queued User ID	Not present		ON-NETWORK
Queued User ID			OFF-NETWORK
Queued User ID	px_MCPTT_User_A_ID	the MCPTT ID of the queued floor participant	
Queue Info			
Queue Position Info	"1"		
Queue Priority Level	"0"		
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	
Floor Indicator			
Floor Indicator	Any allowed value		

5.5.6.11 Floor Ack

Table 5.5.6.11-1: Floor Ack

Derivation Path: 24.380 [10], Table 8.2.13-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPT		
Source			
Source	"2"	The controlling MCPTT function is the source	
Message Type			
Message Type	"10100"	Floor Ack message for Floor Release message which requested acknowledgment	
Track Info	Not present	The MCPTT call does not involve a non-controlling MCPTT function	

5.5.6.12 Connect

Table 5.5.6.12-1: Connect

Derivation Path: 24.380 [10], Table 8.3.4-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPC		
MCPTT Session Identity field			
Session Type	"00000011"	prearranged	
MCPTT Session Identity	px_MCPTT_sesson_B_ID	SIP URI, which identifies the MCPTT session between the MCPTT client and the controlling MCPTT function	
MCPTT Group Identity field	Not Present		PRIVATE-CALL
MCPTT Group Identity field			GROUP-CALL
MCPTT Group Identity	px_MCPTT_Group_A_ID	a URI, which identifies the MCPTT group	
Media Streams			
Media Stream field	"1"	8 bit parameter giving the number of the" m=audio" m-line negotiated in the pre-established session	
Control Channel	"2"	8 bit parameter giving the number of the "m=application" m-line negotiated in the pre-established session	
Warning Text field	Not Present		
Answer State field			
Answer State	"1"	confirmed	
Inviting MCPTT User Identity field			
Inviting MCPTT User Identity	px_MCPTT_User_A_ID	URI, which identifies the inviting MCPTT user	
PCK I_MESSAGE field	Not Present		

5.5.6.13 Disconnect

Table 5.5.6.13-1: Disconnect

Derivation Path: 24.380 [10], Table 8.3.5-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPC		
MCPTT Session Identity field			
Session Type	"00000011"	prearranged	
MCPTT Session Identity	px_MCPTT_sesson_B_ID		

5.5.6.14 Acknowledgement

Table 5.5.6.14-1: Acknowledgement

Derivation Path: 24.380 [10], Table 8.3.6-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPC		
Reason Code			
Reason Code	"0"	Accepted	

5.5.6.15 Map Group To Bearer

Derivation Path: 24.380 [10], Table 8.4.4-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCMC		
MCPTT Group ID	px_MCPTT_Group_A_ID	The group ID of the call	
TMGI			
MBMS Service ID	"0F0F0F"	The selected value is randomly chosen - a 6 digit hexadecimal number between 000000 and FFFFFF (see TS 23.003 [69] subclause 15.2. The coding of the MBMS Service ID is the responsibility of each administration	
MCC	The same value as for PLMN1 specified in Table 5.5.8.1-x	Mobile Country Code	
MNC	The same value as for PLMN1 specified in Table 5.5.8.1-x	Mobile Network Code	
MBMS Subchannel			
Audio m-line Number	"1"	The number of the "m=audio" m-line in the SIP MESSAGE request announcing the MBMS bearer	
Floor m-line Number	"2"	The number of the "m=application" m-line in the SIP MESSAGE request announcing the MBMS bearer. The <Floor m-line Number> value is set to "0" when the same subchannel is used for media and for floor control.	
IP version	"0"	'0' = IP version 4 '1' = IP version 6 All other values are reserved for future use	

Derivation Path: 24.380 [10], Table 8.4.4-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
Floor control Port Number	"9"	The port to be used if the<Floor m-line Number> value is greater than '0'. If the <Floor m-line Number> value is equal to '0', the <Floor control Port Number> value is not included in the MBMS Subchannel field	
Media Port Number	"9"		
IP Address	"0.0.0.0"		

5.5.6.16 Unmap Group To Bearer

Derivation Path: 24.380 [10], Table 8.4.5-1.			
Information Element	**Value/remark**	**Comment**	**Condition**
SSRC	The SSRC of the message sender	The SSRC of the floor control server for on-network and floor arbitrator for off-network. Notation in accordance with subclause 5.5.6.1. Coded as specified in IETF RFC 3550 [76].	
name	MCPT		
MCPTT Group ID	px_MCPTT_Group_A_ID	The group ID of the call	

5.5.7 Default MCPTT group management messages and other information elements

5.5.7.1 MCPTT Group Configuration

Table 5.5.7.1-1: MCPTT Group Configuration Defaults

Derivation Path: TS 24.483 [13], subclause 6.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Node	urn:oma:mo:oma-dm-mcptt-group configuration:1.0	**Group 1**		
Name	"mcptt-group-A-configuration"	Name of configuration file		
Common				
MCPTTGroupID	px_MCPTT_Group_A_ID	Value is a "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1		
MCPTTGroupAlias	px_MCPTT_Group_A_Name	Value is a <display-name> element specified in OMA OMA-TS-XDM_Group-V1_1		
MCPTTGroupMemberList		group member 1		
MCPTTID	px_MCPTT_User_A_ID	Indicates an MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user		
UserPriority	"3"	Indicates the user priority of the MCPTT group member	TS 24.481 [11]	
ParticipantType	px_MCPTT_User_A_ParticipantType	Participant type of the MCPTT group		
MCPTTGroupMemberList		group member 2		
MCPTTID	px_MCPTT_User_B_ID	Indicates an MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user		
UserPriority	"2"	Indicates the user priority of the MCPTT group member	TS 24.481 [11]	
ParticipantType	px_MCPTT_User_B_ParticipantType	Participant type of the MCPTT group		
MCPTTGroupMemberList		group member 3		
MCPTTID	px_MCPTT_User_C_ID	Indicates an MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user		
UserPriority	"1"	Indicates the user priority of the MCPTT group member	TS 24.481 [11]	
ParticipantType	px_MCPTT_User_C_ParticipantType	Participant type of the MCPTT group		
MCPTTGroupOwner	px_MCPTT_Group_A_Owner_Organization	Group's owner (Mission Critical Organisation).		
PreferredVoiceCodec	px_MCPTT_Group_A_preferred_VCodec	Preferred voice codec is a RTP payload. MCPTT clients shall support the AMR-WB codec.	RFC 4566 [27] TS 26.171 [66]	
MCPTTGroupLevel	"0"	Indicates the level within a group hierarchy (only applicable for group-broadcast group).		

Derivation Path: TS 24.483 [13], subclause 6.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
UserLevel	"0"	Indicates the level within user hierarchy (only applicable for user-broadcast group).		
AllowedEmergencyCall	"true"	Indicates whether an MCPTT emergency group call is permitted on the MCPTT group		
AllowedImminentPerilCall	"true"	Indicates whether an MCPTT imminent peril group call is permitted on the MCPTT group		
AllowedEmergencyAlert	"true"	Indicates whether an MCPTT emergency alert is possible on the MCPTT group		
MediaProtectionReq	"true"	Indicates whether confidentiality and integrity of media is required on the MCPTT group		
FloorControlProtectionReq	"true"	Indicates whether confidentiality and integrity of floor control signalling is required on the MCPTT group		
MediaProtectionSecurityMaterial	MIKEY-SAKKE I_MESSAGE as defined in Table 5.5.9.1-3	The security material for group media protection.	TS 33.179 [15]	
OffNetwork				
MCPTTGroupParameter				
ProSeLayer2GroupID	px_Group_A_ProSeLayer2GroupID	Indicates the Prose layer-2 group ID	TS 23.303 [68]	
IPMulticastAddress	"0.0.0.0"	Indicates the ProSe group IP multicast address	TS 23.303 [68]	
RelayServiceCode	"123456"	Indicates the connectivity service that the ProSe UE-to-network relay provides to public safety applications	TS 23.303 [68]	
IPVersions	"IPv4"	Indicates whether IPv4 or IPv6 is used for the MCPTT group	TS 23.303 [68]	
EmergencyCallCancel	"65535"	Indicates the timeout value for the cancellation of an in progress emergency for an MCPTT group call. Values: 0-65535 s		
ImminentPerilCallCancel	"65535"	Indicates the timeout value for the cancellation of an in progress imminent peril for an MCPTT group call. Values: 0-65535 s		
HangTime	"5"	Indicates the group call hang timer. Values: 0-65535 s		
MaxDuration	"60"	Indicates the max duration of group calls. Values: 0-65535 s		
QueueUsage	"true"	Indicates if queuing is enabled or not		

Derivation Path: TS 24.483 [13], subclause 6.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
DefaultPPPP				
GroupCallSignalling	"1"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
GroupCallMedia	"1"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
EmerGroupCallSignalling	"8"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
EmerGroupCallMedia	"8"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
ImPerilGroupCallSignalling	"7"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
ImPerilGroupCallMedia	"7"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
Node	urn:oma:mo:oma-dm-mcptt-group configuration:1.0	**Group 2**		
Name	"mcptt-group-D-configuration"	Name of configuration file		
Common				
MCPTTGroupID	px_MCPTT_Group_D_ID	Value is a "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1		
MCPTTGroupAlias	px_MCPTT_Group_D_Name	Value is a <display-name> element specified in OMA OMA-TS-XDM_Group-V1_1		
MCPTTGroupMemberList		group member 1		
MCPTTID	px_MCPTT_User_A_ID	Indicates an MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user		
UserPriority	"3"	Indicates the user priority of the MCPTT group member	TS 24.481 [11]	
ParticipantType	px_MCPTT_User_A_ParticipantType	Participant type of the MCPTT group		
MCPTTGroupMemberList		group member 2		
MCPTTID	px_MCPTT_User_B_ID	Indicates an MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user		
UserPriority	"2"	Indicates the user priority of the MCPTT group member	TS 24.481 [11]	
ParticipantType	px_MCPTT_User_B_ParticipantType	Participant type of the MCPTT group		
MCPTTGroupOwner	px_MCPTT_Group_D_Owner_Organization	Group's owner (Mission Critical Organisation).		
PreferredVoiceCodec	px_MCPTT_Group_D_preferred_VCodec	Preferred voice codec is a RTP payload. MCPTT clients shall support the AMR-WB codec.	RFC 4566 [27] TS 26.171 [66]	

Derivation Path: TS 24.483 [13], subclause 6.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
MCPTTGroupLevel	"0"	Indicates the level within a group hierarchy (only applicable for group-broadcast group).		
UserLevel	"0"	Indicates the level within user hierarchy (only applicable for user-broadcast group).		
AllowedEmergencyCall	"false"	Indicates whether an MCPTT emergency group call is permitted on the MCPTT group		
AllowedImminentPerilCall	"false"	Indicates whether an MCPTT imminent peril group call is permitted on the MCPTT group		
AllowedEmergencyAlert	"false"	Indicates whether an MCPTT emergency alert is possible on the MCPTT group		
MediaProtectionReq	"true"	Indicates whether confidentiality and integrity of media is required on the MCPTT group		
FloorControlProtectionReq	"true"	Indicates whether confidentiality and integrity of floor control signalling is required on the MCPTT group		
MediaProtectionMaterial	MIKEY-SAKKE I_MESSAGE as defined in Table 5.5.9.1-1	The security material for group media protection.	TS 33.179 [15]	
OffNetwork				
MCPTTGroupParameter				
ProSeLayer2GroupID	px_MCPTT_Group_D_ ProSeLayer2GroupID	Indicates the Prose layer-2 group ID	TS 23.303 [68]	
IPMulticastAddress	"0.0.0.0"	Indicates the ProSe group IP multicast address	TS 23.303 [68]	
RelayServiceCode	"123456"	Indicates the connectivity service that the ProSe UE-to-network relay provides to public safety applications	TS 23.303 [68]	
IPVersions	"IPv4"	Indicates whether IPv4 or IPv6 is used for the MCPTT group	TS 23.303 [68]	
EmergencyCallCancel	"65535"	Indicates the timeout value for the cancellation of an in progress emergency for an MCPTT group call. Values: 0-65535 s		
ImminentPerilCallCancel	"65535"	Indicates the timeout value for the cancellation of an in progress imminent peril for an MCPTT group call. Values: 0-65535 s		
HangTime	"5"	Indicates the group call hang timer. Values: 0-65535 s		

Derivation Path: TS 24.483 [13], subclause 6.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
MaxDuration	"60"	Indicates the max duration of group calls. Values: 0-65535 s		
QueueUsage	"true"	Indicates if queuing is enabled or not		
DefaultPPPP				
GroupCallSignalling	"1"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
GroupCallMedia	"1"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
EmerGroupCallSignalling	"8"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
EmerGroupCallMedia	"8"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
ImPerilGroupCallSignalling	"7"	Indicates the default ProSe Per-Packet Priority (PPPP) value		
ImPerilGroupCallMedia	"7"	Indicates the default ProSe Per-Packet Priority (PPPP) value		

5.5.8 Default MCPTT configuration management messages and other information elements

5.5.8.1 MCPTT Initial UE Configuration

Table 5.5.8.1-1: MCPTT Initial UE Configuration Defaults

Derivation Path: TS 24.483 [13], subclause 8.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Node	"urn:oma:mo:oma-dm-mcptt-ue-initial-configuration:1.0"	Base node		
Name	"mcptt-client-A-init-config"	Name of configuration file		
Ext	px_MCPTT_vendor_specific_information_init_configC			
DefaultUserProfile				
UserID	px_MCPTT_User_A_ID	Default User Identity		
UserProfileIndex	"0"	Values 0-255. Indicates selected user profile		
OnNetwork				
GMSURI	px_MCPTT_GMSURI	The group management service URI information which contains the public service identity for performing subscription proxy function of the GMS	TS 23.003 [69]	
GroupCreationXUI	px_MCPTT_GroupCreationXUI	Indicates the group creation XUI information for creation of groups	TS 23.003 [69]	
GMSXCAPRootURI	px_MCPTT_GMSXCAPRootURI	Indicates the group management server XCAP Root URI information	TS 23.003 [69]	
CMSXCAPRootURI	px_MCPTT_CMSXCAPRootURI	Indicates the configuration management server XCAP Root URI information	TS 23.003 [69]	
Timers				
T100	"2"	Values 0-255 sec	TS 24.380 [10]	
T101	"2"	Values 0-255 sec	TS 24.380 [10]	
T103	"5"	Values 0-255 sec	TS 24.380 [10]	
T104	"2"	Values 0-255 sec	TS 24.380 [10]	
T132	"3"	Values 0-255 sec	TS 24.380 [10]	
HPLMN				
PLMN	PLMN1	the PLMN on which the UE is allowed for MCPTT services. Public Land Mobile Network is uniquely identified by its PLMN identifier; consists of Mobile Country Code (MCC) and Mobile Network Code (MNC) and are defined by the operator. NOTE: PLMN1 shall be the PLMN of the Cell on which the UE is camped during testing.	TS 23.003 [69]	
Service		Node indicates the MCPTT related services on a per HPLMN basis		

Derivation Path: TS 24.483 [13], subclause 8.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
MCPTTToConRef		interior node contains the configuration parameters for establishment of the PDN connection for the **MCPTT service** on a per HPLMN basis		
ConRef	px_MCS_ALL_APN	<A network access point object> linkage to the connectivity parameters		
MCCommonCoreToConRef		interior node contains the configuration parameters for establishment of the PDN connection for the **MC common core service** on a per HPLMN basis		
ConRef	px_MCPTT_ALL_APN	<A network access point object> linkage to the connectivity parameters		
MCIDMToConRef		interior node contains the configuration parameters for establishment of the PDN connection for the **MC identity management service** on a per HPLMN basis		
ConRef	px_MCPTT_ALL_APN	<A network access point object> linkage to the connectivity parameters		
VPLMN				
PLMN	PLMN2	VPLMN configuration for another PLMN which can be used by the UE to access MCPTT service NOTE: PLMN2 shall be a different PLMN to PLMN1 of a Cell to which the UE will move during testing when specified in a test case.		
Service		Node indicates the MCPTT related services on the VPLMN		
MCPTTToConRef		interior node contains the configuration parameters for establishment of the PDN connection for the **MCPTT service** on a per VPLMN and HPLMN basis		
ConRef	px_MCPTT_ALL_APN	<A network access point object> linkage to the connectivity parameters		

Derivation Path: TS 24.483 [13], subclause 8.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
MCCommonCoreToConRef		interior node contains the configuration parameters for establishment of the PDN connection for the **MC common core service** on a per VPLMN and HPLMN basis		
ConRef	px_MCPTT_ALL_APN	<A network access point object> linkage to the connectivity parameters		
MCIDMToConRef		interior node contains the configuration parameters for establishment of the PDN connection for the **MC identity management service** on a per VPLMN and HPLMN basis		
ConRef	px_MCPTT_ALL_APN	<A network access point object> linkage to the connectivity parameters		
AppServerInfo				
IDMSAuthEndpoint	px_MCPTT_IDMSAuthEndpoint	Identity management server authorisation endpoint identity information	TS 23.003 [69]	
IDMSTokenEndpoint	px_MCPTT_IDMSTokenEndpoint	Identity management server token endpoint identity information	TS 23.003 [69]	
HTTPProxy	not present	No HTTP Proxy	TS 23.003 [69]	
GMS	px_MCPTT_GMS	Indicates the group management server identity information	TS 23.003 [69]	
CMS	px_MCPTT_CMS	Indicates the configuration management server identity information	TS 23.003 [69]	
KMS	px_MCPTT_KMS	Indicates the key management server identity information	TS 23.003 [69]	
TLSTunnelAuthMethod				
Mutual	"false"	Indicates whether mutual authentication is used for the TLS tunnel authentication false=one-way authentication based on the server certificate is used		
X509	""	the X.509 certificate for mutual authentication for the TLS tunnel authentication		
Key	""	pre-shared key for mutual authentication for the TLS tunnel authentication		
IntegrityProtection	"true"	Indicates whether integrity protection is enabled		

Derivation Path: TS 24.483 [13], subclause 8.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
ConfidentialityProtection	"true"	Indicates whether integrity protection is enabled		
OffNetwork				
Timers				
TFG1	"150"	Indicates the timer for wait for call announcement; Values: 0-65535 ms	TS 24.379 [9]	
TFG2	"2000"	Indicates the timer for call announcement; Values: 0-65535 ms	TS 24.379 [9]	
TFG3	"40"	Indicates the timer for call probe retransmission; Values: 0-65535 ms	TS 24.379 [9]	
TFG4	"20"	Indicates the timer for waiting for the MCPTT user; Values: 0-60 s	TS 24.379 [9]	
TFG5	"2"	Indicates the timer for not present incoming call announcements; Values: 0-255 s	TS 24.379 [9]	
TFG11	"3000"	Indicates the timer for MCPTT emergency end retransmission; Values: 0-65535 ms	TS 24.379 [9]	
TFG12	"3000"	Indicates the timer for MCPTT imminent peril end retransmission; Values: 0-65535 ms	TS 24.379 [9]	
TFG13	"1"	Indicates the timer for implicit priority downgrade; Values: 0-255 s	TS 24.379 [9]	
TFG14	"1"	Indicates the MCPTT timer for implicit priority downgrade (imminent peril); Values: 0-255 s	TS 24.379 [9]	
TFP1	"2000"	Indicates the timer for private call request retransmission; Values: 0-65535 ms	TS 24.379 [9]	
TFP2	"5000"	Indicates the timer for waiting for call response message; Values: 0-65535 ms	TS 24.379 [9]	
TFP3	"2000"	Indicates the timer for private call release retransmission; Values: 0-65535 ms	TS 24.379 [9]	
TFP4	"5000"	Indicates the timer for private call release retransmission; Values: 0-65535 ms	TS 24.379 [9]	
TFP5	"30"	Indicates the timer for call release; Values: 0-600 s	TS 24.379 [9]	
TFP6	"3000"	Indicates the timer for MCPTT emergency private call cancel retransmission; Values: 0-65535 ms	TS 24.379 [9]	

Derivation Path: TS 24.483 [13], subclause 8.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
TFP7	"6"	Indicates the timer for waiting for any message with same call identifier; Values: 0-255 s	TS 24.379 [9]	
TFB1	"300"	Indicates the timer for max duration; Values: 0-600 s	TS 24.379 [9]	
TFB2	"10"	Indicates the timer for max duration; Values: 0-10 s	TS 24.379 [9]	
TFB3	"20"	Indicates the timer for waiting for the MCPTT user; Values: 0-60 s	TS 24.379 [9]	
T201	"1000"	Indicates the timer for floor request; Values: 0-65535 ms	TS 24.380 [10]	
T203	"5"	Indicates the timer for end of RTP media; Values: 0-255 s	TS 24.380 [10]	
T204	"5"	Indicates the timer for floor queue position request; Values: 0-255 s	TS 24.380 [10]	
T205	"1"	Indicates the timer for floor granted request; Values: 0-255 s	TS 24.380 [10]	
T230	"10"	Indicates the timer for inactivity; Values: 0-255 s	TS 24.380 [10]	
T233	"10"	Indicates the timer for pending user action; Values: 0-255 s	TS 24.380 [10]	
TFE1	"30"	Indicates the timer for MCPTT emergency alert; Values: 0-65535 s	TS 24.379 [9]	
TFE2	"10"	Indicates the timer for MCPTT emergency alert re-transmission; Values: 0-10 s	TS 24.379 [9]	
Counters				
CFP1	"3"	Indicates the counter for private call request retransmission	TS 24.379 [9]	
CFP3	"5"	Indicates the counter for private call release retransmission	TS 24.379 [9]	
CFP4	"2"	Indicates the counter for private call accept retransmission	TS 24.379 [9]	
CFP6	"2"	Indicates the counter for private call accept retransmission	TS 24.379 [9]	
CFP11	"2"	Indicates the counter for MCPTT group call emergency end retransmission	TS 24.379 [9]	
CFP12	"2"	Indicates the counter for MCPTT imminent peril call emergency end retransmission	TS 24.379 [9]	
C201	"3"	Indicates the counter for floor request	TS 24.379 [9]	

Derivation Path: TS 24.483 [13], subclause 8.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
C204	"2"	Indicates the counter for floor queue position request	TS 24.379 [9]	
C205	"4"	Indicates the counter for floor granted request	TS 24.379 [9]	

5.5.8.2 MCPTT UE Configuration

Table 5.5.8.2-1: MCPTT UE Configuration Defaults

Derivation Path: TS 24.483 [13], subclause 4.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Node	"urn:oma:mo:oma-dm-mcptt-ue-configuration:1.0"	Base node		
Name	"mcptt-client-A-config"	Name of configuration file		
Ext	px_MCPTT_vendor_specific_information_config			
Common		For on-network operation and off-network operation		
PrivateCall				
MaxCallN10	"2"	Indicates the maximum number of private calls		
MCPTTGroupCall				
MaxCallN4	"3"	Indicates the maximum number of simultaneous group calls		
MaxTransmissionN5	"5"	Indicates the maximum number of transmissions in a group		
PrioritizedMCPTTGroup		One prioritised group		
MCPTTGroupID	px_MCPTT_Group_A_ID	Value is a "uri" attribute specified in OMA OMA-TS-XDM_Group-V1_1 that indicates the group id.		
MCPTTGroupPriority	"7"	Indicates the requested presentation priority of group call; Values: 0-7 "7"=the top priority among groups		
OnNetwork		Only for on-network operation		
RelayService	"true"	Indicates the authorisation to use a relay service		
IPv6Preferred	"false"	Indicates whether IPv6 is preferred over IPv4 for on-network operation when the MCPTT UE has both IPv4 and IPv6 host configuration.		
RelayedMCPTTGroup				
MCPTTGroupID	px_MCPTT_Group_A_ID	One allowed relayed MCPTT group		
RelayServiceCode	"123456"	Identifies a connectivity service the ProSe UE-to-Network Relay provides to Public Safety applications; 24-bit value	TS 23.303 [68]	

5.5.8.3 MCPTT User Profile

Table 5.5.8.3-1: MCPTT User Profile Defaults

Derivation Path: TS 24.483 [13], subclause 5.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Node	"urn:oma:mo:oma-dm-mcptt-user-profile:1.0"	Base node		
Name	"mcptt-user-A-profile"	Name of User Profile file		
Ext	px_MCPTT_vendor_specific_information_user_profile			
Common				
MCPTTUserID	px_MCPTT_User_A_ID	MCPTT user identity (MCPTT ID) which is a globally unique identifier within the MCPTT service that represents the MCPTT user		
MCPTTUserProfileIndex	"0"	Index for the particular MCPTT user profile		
MCPTTUserProfileName	px_MCPTT_User_A_Profile_Name	Profile name for the MCPTT user		
PreSelectedIndication	not present		TS 23.179 [8]	
UserAlias	px_MCPTT_User_A_Alias	Alphanumeric aliases of MCPTT user		
AuthorisedAlias	"false"	Indicates authorisation to create and delete aliases of other MCPTT users		
ParticipantType	px_MCPTT_User_A_ParticipantType	Participant type of the MCPTT user		
Organization	px_MCPTT_User_A_Organization	Indicates the organization an MCPTT user belongs to		
PrivateCall				
Authorised	"true"	Indicates the authorisation to make a MCPTT private call		
AuthorisedAny	"true"	indicates the authorisation to make a MCPTT private call to any MCPTT user		
UserList		User 1		
Entry				
MCPTTID	px_MCPTT_User_B_ID	MCPTT user(s) who can be called in a MCPTT private call		
DiscoveryGroupID	"1234"	Discovery group ID in the ProSe discovery procedures	TS 23.303 [68]	
UserInfoID	"5555"	Prose user Info ID in the ProSe discovery procedures	TS 23.303 [68]	
DisplayName	"User B Name"	a human readable name for this User		
UserList		User 2		
Entry				
MCPTTID	px_MCPTT_User_C_ID	MCPTT user(s) who can be called in a MCPTT private call		
DiscoveryGroupID	"1234"	Discovery group ID in the ProSe discovery procedures	TS 23.303 [68]	
UserInfoID	"6666"	ProSe user Info ID in the ProSe discovery procedures	TS 23.303 [68]	
DisplayName	"User C Name"	a human readable name for this User		

Derivation Path: TS 24.483 [13], subclause 5.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
ManualCommence	"true"	Indicates the authorisation to make a MCPTT private call with manual commencement		
AutoCommence	"true"	Indicates the authorisation to make a MCPTT private call with automatic commencement		
AutoAnswer	"true"	Indicates the authorisation of MCPTT user to force automatic answer for a MCPTT private call		
FailRestrict	"false"	Indicates the authorisation to restrict the provision of a notification of call failure reason for a MCPTT private call		
MediaProtection	"true"	Indicates authorisation to protect confidentiality and integrity of media for MCPTT private calls		
FloorControlProtection	"true"	Indicates authorisation to protect confidentiality and integrity of floor control signalling for MCPTT private calls.		
EmergencyCall				
Authorised	"true"	Indicates the authorisation to make an MCPTT emergency private call.		
CancelPriority	"true"	Indicates the authorisation to cancel emergency priority in an MCPTT emergency private call by an authorised MCPTT user		
MCPTTPrivateRecipient				
Entry				
ID	px_MCPTT_User_B_ID	The MCPTT private recipient for an MCPTT emergency private call		
DiscoveryGroupID	"1234"	Discovery group ID in the ProSe discovery procedures		
UserInfoID	"5555"	ProSe user Info ID in the ProSe discovery procedures		
DisplayName	"User B Name"	a human readable name for this User		
Usage	"UsePreConfigured"	Indicates the criteria to determine when initiation of an MCPTT emergency private call uses the MCPTT private recipient ID.		
MCPTTGroupCall				

Derivation Path: TS 24.483 [13], subclause 5.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
MaxSimultaneousCallsN6	"3"	Indicates the maximum number of simultaneously received MCPTT group calls		
EmergencyCall				
Enabled	"true"	Indicates the authorisation to make an MCPTT emergency group call functionality enabled for MCPTT user		
MCPTTGroupInitiation				
Entry				
GroupID	px_MCPTT_Group_A_ID	The group used upon certain criteria on initiation of an MCPTT emergency group call		
DisplayName	px_MCPTT_Group_A_Namenot present	The display name for group used for emergency		
Usage	"UseCurrentlySelectedGroup"	Use currently selected MCPTT group for an on-network MCPTT emergency group call		
CancelMCPTTGroup	"true"	Indicates the authorisation to cancel an in progress MCPTT emergency call associated with a group.		
ImminentPerilCall				
Authorised	"true"	Indicates the authorisation to make an Imminent Peril group call		
Cancel	"true"	Indicates the authorisation for in-progress MCPTT imminent peril cancelation		
MCPTTGroupInitiation				
Entry		Multiple entries [x]; single default entry		
GroupID	px_MCPTT_Group_A_ID	the group used on initiation of an MCPTT imminent peril group call.		
DisplayName	px_MCPTT_Group_A_Namenot present	display name for group used for the imminent peril call		
Usage	"UseCurrentlySelectedGroup"	Use currently selected MCPTT group for an on-network MCPTT imminent peril group call		
EmergencyAlert				
Authorised	"true"	Indicates the authorisation to activate an MCPTT emergency alert		
Cancel	"true"	Indicates the authorisation to cancel an MCPTT emergency alert		

Derivation Path: TS 24.483 [13], subclause 5.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Entry				
ID	px_MCPTT_Group_A_ID	Indicates the MCPTT group used upon certain criteria on initiation of an MCPTT emergency alert.		
DisplayName	px_MCPTT_Group_A_Namenot present	Optional; name of emergency alert group		
Usage	"UseCurrentlySelectedGroup"	Use currently selected MCPTT group for emergency alert		
Priority	"10"	Indicates the priority of the MCPTT group calls, 0-255		
MCPTTGroupBroadcast				
Authorised	"true"	Indicates the authorisation to create a user-broadcast group		
UserBroadcast				
Authorised	"true"	Indicates the authorisation to create a user-broadcast group		
OnNetwork				
MCPTTGroupList		Group 1 the MCPTT user is allowed to affiliate to		
Entry				
MCPTTGroupID	px_MCPTT_Group_A_ID	The MCPTT group ID for the on-network MCPTT group that the MCPTT user is allowed to affiliate to.		
DisplayName	px_MCPTT_Group_A_Name	The display name for the group		
MCPTTGroupList		Group 2 the MCPTT user is allowed to affiliate to		
Entry				
MCPTTGroupID	px_MCPTT_Group_D_ID	The MCPTT group ID for the on-network MCPTT group that the MCPTT user is allowed to affiliate to.		
DisplayName	px_MCPTT_Group_D_Name	The display name for the group		
ImplicitAffiliations		Group 1 the MCPTT user is implicitly affiliated to		
Entry		Multiple entries [x]; single default entry		
MCPTTGroupID	px_MCPTT_Group_A_ID	indicates a MCPTT group ID to which the MCPTT user is implicitly affiliated to		
DisplayName	px_MCPTT_Group_A_Name	display name for implicitly affiliated group		
AllowedRegroup	"true"	Indicates whether the MCPTT user is authorised to perform dynamic regrouping operations		

Derivation Path: TS 24.483 [13], subclause 5.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
AllowedPresenceStatus	"true"	Indicates the presence status on the network of this MCPTT user is available		
AllowedPresence	"true"	Indicates whether the MCPTT user is authorised to obtain whether a particular MCPTT User is present on the network		
EnabledParticipation	"true"	Indicates whether the MCPTT user is allowed to participate in MCPTT private calls that they are invited to		
AllowedTransmission	"true"	Indicates whether the MCPTT user is authorised to override transmission in a MCPTT private call		
AllowedManualSwitch	"true"	Indicates whether the MCPTT user is authorised to manually switch to off-network operation while in on-network operation		
PrivateCall				
EmergencyAlert				
Entry				
ID	px_MCPTT_User_B_ID	Indicates the default MCPTT user ID to be used upon certain criteria on initiation of an MCPTT private emergency alert for on-network		
DisplayName	px_MCPTT_User_A_Alias	The display name corresponding to private emergency call id		
Usage	"UsePreConfigured"	Indicates the criteria to determine when initiation of an MCPTT emergency private call uses the MCPTT private recipient ID.		
OffNetwork				
Authorised	"true"	Indicates the authorisation for off-network services		
MCPTTGroupInfo		Group 1		
Entry				
MCPTTGroupID	px_MCPTT_Group_A_ID	Indicates an off-network MCPTT group for use by an MCPTT user		
DisplayName	px_MCPTT_Group_A_Name	The display name corresponding to off-network group id		
AllowedListen	"false"	Indicates whether the MCPTT user is allowed to listen both overriding and override		

Derivation Path: TS 24.483 [13], subclause 5.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
AllowedTransmission	"false"	Indicates whether the MCPTT user is allowed to transmit in case of override (overriding and/or overridden)		
EmergencyCallChange	"true"	Indicates the authorisation for a participant to change an off-network group call in-progress to an off-network MCPTT emergency group call		
ImminentPerilCallChange	"true"	Indicates the authorisation for a participant to change an off-network group call in-progress to an off-network MCPTT imminent peril group call		
UserInfoID	"5555"	ProSe user info ID	TS 23.303 [68]	
Status	"true"	indicates whether this MCPTT user profile is enabled or disabled		

5.5.8.4 MCPTT Service Configuration

Table 5.5.8.4-1: MCPTT Service Configuration Defaults

Derivation Path: TS 24.483 [13], subclause 7.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
Node	"urn:oma:mo:oma-dm-mcptt-service configuration:1.0"			
Name	"mcptt-service-configuration"	Name of configuration file		
Ext	px_MCPTT_vendor_specific_information_service_conf			
Common				
BroadcastMCPTTGroupCall				
NumLevelGroupHierarchy	"1"	Indicates the number of levels of group hierarchy for group-broadcast groups		
NumLevelUserHierarchy	"1"	Indicates the number of levels of user hierarchy for user-broadcast groups		
MinLengthAliasID	"2"	Indicates minimum length of an alphanumeric identifier (i.e., alias)		
OffNetwork				
PrivateCall				
MaxDuration	"60"	Indicates max private call (with floor control) duration. Values: 0-65535 s		
HangTime	"5"	Indicates hang timer for private calls (with floor control). Values: 0-65535 s		
CancelTimeout	"5"	Indicates timeout value for the cancellation of an in progress emergency for an MCPTT private call. Values: : 0-65535 s		
EmergencyCall				
MCPTTGroupTimeout	"5"	Indicates time limit for an in progress MCPTT emergency call related to an MCPTT group. Values: 0-65535 s		
NumLevelHierarchy	"4"	Indicates the number of levels of hierarchy for floor control override in off-network. Values: 4-256		
TransmitTimeout	"60"	Indicates transmit time limit from a single request to transmit in a group or private call. Values: 0-65535 s		
TransmissionWarning	"50"	Indicates configuration of warning time before time limit of transmission is reached (off-network). Values: 0-255 s		
HangTimeWarning	"4"	Indicates configuration of warning time before hang time is reached (off-network). Values: Values: 0-255 s		

Derivation Path: TS 24.483 [13], subclause 7.2				
Information Element	**Value/remark**	**Comment**	**Reference**	**Condition**
DefaultPPPP				
PrivateCallSignalling	"1"	Indicates the default ProSe Per-Packet Priority (PPPP) value	TS 23.303 [68]	
PrivateCallMedia	"1"	Indicates the default ProSe Per-Packet Priority (PPPP) value	TS 23.303 [68]	
EmerPrivateCallSignalling	"8"	Indicates the default ProSe Per-Packet Priority (PPPP) value	TS 23.303 [68]	
EmergencyPrivateCallMedia	"8"	Indicates the default ProSe Per-Packet Priority (PPPP) value	TS 23.303 [68]	
LogMetadata	"true"	Indicates whether an MCPTT emergency group call is permitted on the MCPTT group		

5.5.9 Default miscellaneous messages and other information elements

5.5.9.1 MIKEY-SAKKE I_MESSAGE

Table 5.5.9.1-1: MIKEY-SAKKE I_MESSAGE (CSK distribution)

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
MIKEY Common Header {	Any		
version	‘00000001’B		
Data Type	‘00011010’B	SAKKE msg (26)	
Next payload	‘00000101’B	Next payload is timestamp	
V	‘0’B		
PRF func	‘0000001’B	PRF-HMAC-SHA-256	
CSB ID	CSK-ID	32 bits See TS 33.179 [15] subclause F.2.	
#CS	‘00000001’B	the number of crypto sessions in the CS ID map info.	
CS ID map type	2	GENERIC-ID	
CS ID map info {			
CS ID	‘00000001’B	the CS ID of the crypto session 8 bits	
Prot type	0	SRTP the security protocol to be used for the crypto session	
S	1	the ROC and SEQ fields are provided	
#P	1	the number of security policies provided for the crypto session	
Ps {		lists the policies for the crypto session	
Policy_no_1	'00000001'B	a policy_no that corresponds to the policy_no of a SP payload	
}			
Session Data Length		16 bits the length of Session Data (in bytes). For the Prot type SRTP, Session Data MAY be omitted in the initial message (length = 0), but it MUST be provided in the response message.	
Session Data {		session data for the crypto session	
SSRC		specifies the SSRC that MUST be used for the crypto session	
ROC		current/initial rollover counter. If the session has not started, this field is set to '0'	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
SEQ		current/initial sequence number	
}			
SPI Length		SPI MAY be omitted in the initial message (length = 0), but it has to be provided in the response message	
SPI		the SPI (or MKI) corresponding to the session key to (initially) be used for the crypto session. Other keys can be used.	
}			
}			
Timestamp Payload (T) {			
Next payload	‘00001011’B	Next payload is RAND	
TS Type	‘00000011’B	NTP-UTC-32 (3)	
TS Value	3710502000	A randomly chose value = Corresponds to 31/07/2017, 17:00:00. The time of issue represented by the number of seconds since 0h on 1 January 1900 with respect to the Coordinated Universal Time (UTC)	
}			
RAND Payload {			
Next payload	‘00001110’B	Next payload is IDRi	
RAND len	‘00010000’B	It should be at least 16 Bytes	
RAND	128-bit random number		
}			
IDRi payload {			
Next payload	‘00001110’B	Next payload is IDRr	
ID Role	1	Initiator (IDRi)	
ID Type	1	URI	
ID len	Length of ID Data		
ID data	px_MCPTT_User_A_ID	MCPTT ID See TS 33.179 [15] clause E.3	
}			
IDRr payload {			
Next payload	‘00001110’B	Next payload is IDRkmsi	
ID Role	2	Responder (IDRr)	
ID Type	1	URI	
ID len	Length of ID Data		
ID data	px_MCPTT_Server_A_URI	MDSI of the MCPTT Domain	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
}			
IDRkmsi payload {			
Next payload	‘00001110’B	Next payload is IDRkmsr	
ID Role	6	Initiator's KMS (IDRkmsi)	
ID Type	1	URI	
ID len	Length of ID Data		
ID data	px_MCPTT_KMS	the URI of the MCPTT KMS used by the initiating user	
}			
IDRkmsr payload {			
Next payload	‘00001010’B	Next payload is Security Properties	
ID Role	7	Responder's KMS (IDRkmsr)	
ID Type	1	URI	
ID len	Length of ID Data		
ID data	px_MCPTT_KMS	the URI of the MCPTT KMS used by the terminating user	
}			
Security Properties payload {		When not included the content specified below is assumed	
Next payload	‘00011010’B	Next payload is SAKKE (26)	
Policy no	'00000001'B	Random nr	
Prot type	0	SRTP	
Policy param length			
Policy param {			
{			
Type	0	Encryption Algorithm	
length			
value	6	AES-GCM	
}			
{			
Type	1	Session encryption key length	
length			
value	16	16 octets	
}			
{			
Type	4	Session salt key length	
length			
value	12	12 octets	
}			
{			
Type	5	SRTP PRF	
length			
value	0	AES-CM	
}			
{			
Type	6	Key derivation rate	
length			

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
value	0	No session key refresh.	
}			
{			
Type	13	ROC transmission rate	
length			
value	1	ROC transmitted in every packet.	
}			
{			
Type	18	SRTP Authentication tag length	
length			
value	4	4 octets for transmission of ROC	
}			
{			
Type	19	SRTCP Authentication tag length	
length			
value	0	ROC need not be transmitted in SRTCP.	
}			
{			
Type	20	AEAD authentication tag length	
length			
value	16	16 octets	
}			
}			
}			
SAKKE payload {			
Next payload	‘00000100’B	Next payload is SIGN	
SAKKE params {	1	RFC 6509 [23], Appendix A	
n	128		
p	997ABB1F 0A563FDA 65C61198 DAD0657A 416C0CE1 9CB48261 BE9AE358 B3E01A2E F40AAB27 E2FC0F1B 228730D5 31A59CB0 E791B39F F7C88A19 356D27F4 A666A6D0 E26C6487 326B4CD4 512AC5CD 65681CE1 B6AFF4A8 31852A82 A7CF3C52 1C3C09AA 9F94D6AF 56971F1F FCE3E823 89857DB0 80C5DF10 AC7ACE87 666D807A FEA85FEB		

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
q	265EAEC7 C2958FF6 99718466 36B4195E 905B0338 672D2098 6FA6B8D6 2CF8068B BD02AAC9 F8BF03C6 C8A1CC35 4C69672C 39E46CE7 FDF22286 4D5B49FD 2999A9B4 389B1921 CC9AD335 144AB173 595A0738 6DABFD2A 0C614AA0 A9F3CF14 870F026A A7E535AB D5A5C7C7 FF38FA08 E2615F6C 203177C4 2B1EB3A1 D99B601E BFAA17FB		
Px	53FC09EE 332C29AD 0A799005 3ED9B52A 2B1A2FD6 0AEC69C6 98B2F204 B6FF7CBF B5EDB6C0 F6CE2308 AB10DB90 30B09E10 43D5F22C DB9DFA55 718BD9E7 406CE890 9760AF76 5DD5BCCB 337C8654 8B72F2E1 A702C339 7A60DE74 A7C1514D BA66910D D5CFB4CC 80728D87 EE9163A5 B63F73EC 80EC46C4 967E0979 880DC8AB EAE63895		
Py	0A824906 3F6009F1 F9F1F053 3634A135 D3E82016 02990696 3D778D82 1E141178 F5EA69F4 654EC2B9 E7F7F5E5 F0DE55F6 6B598CCF 9A140B2E 416CFF0C A9E032B9 70DAE117 AD547C6C CAD696B5 B7652FE0 AC6F1E80 164AA989 492D979F C5A4D5F2 13515AD7 E9CB99A9 80BDAD5A D5BB4636 ADB9B570 6A67DCDE 75573FD7 1BEF16D7		
g	66FC2A43 2B6EA392 148F1586 7D623068 C6A87BD1 FB94C41E 27FABE65 8E015A87 371E9474 4C96FEDA 449AE956 3F8BC446 CBFDA85D 5D00EF57 7072DA8F 541721BE EE0FAED1 828EAB90 B99DFB01 38C78433 55DF0460 B4A9FD74 B4F1A32B CAFA1FFA D682C033 A7942BCC E3720F20 B9B7B040 3C8CAE87 B7A0042A CDE0FAB3 6461EA46		
Hash	SHA-256	(defined in [FIPS180-3]	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
}			
ID scheme	'URI Scheme'		
SAKKE data length		16 bits length of SAKKE data (in bytes)	
..SAKKE data	encapsulate the CSK to the UID generated from the MDSI of the MCPTT Domain		
}			
SIGN (ECCSI) payload {			
Next payload	‘00000000’B	This is the last payload	
S type	2	ECCSI signature	
S data		contains a signature in the SIGN payload, which is based on the user identity (UID) of the MCPTT User. This identity is derived from the MCPTT ID of the user and a time-related parameter (e.g. the current year and month).	
}			

Table 5.5.9.1-2: MIKEY-SAKKE I_MESSAGE (Private call)

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
MIKEY Common Header {	Any		
version	‘00000001’B		
Data Type	‘00011010’B	SAKKE msg (26)	
Next payload	‘00000101’B	Next payload is timestamp	
V	‘0’B		
PRF func	‘0000001’B	PRF-HMAC-SHA-256	
CSB ID	'0001xxxx ... xxxxxxxx'B	32-bit PCK-ID The 4 most significant bits of the PCK-ID indicate the purpose of the PCK is to protect Private call communications, the other 28-bits are randomly generated	
#CS	‘00000001’B	the number of crypto sessions in the CS ID map info.	
CS ID map type	2	GENERIC-ID	
CS ID map Info {			
CS ID	‘00000010’B	the CS ID of the crypto session	
Prot type	0	the security protocol to be used for the crypto session	
S	1	the ROC and SEQ fields are provided	
#P	1	the number of security policies provided for the crypto session	
Ps {		lists the policies for the crypto session	
Policy_no_1	'00000001'B	a policy_no that corresponds to the policy_no of a SP payload	
}			
Session Data Length		16 bits the length of Session Data (in bytes). For the Prot type SRTP, Session Data MAY be omitted in the initial message (length = 0), but it MUST be provided in the response message.	
Session Data {		session data for the crypto session	
SSRC		specifies the SSRC that MUST be used for the crypto session	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
ROC		current/initial rollover counter. If the session has not started, this field is set to '0'	
SEQ		current/initial sequence number	
}			
SPI Length		SPI MAY be omitted in the initial message (length = 0), but it MUST be provided in the response message	
SPI		the SPI (or MKI) corresponding to the session key to (initially) be used for the crypto session. Other keys can be used.	
}			
}			
Timestamp Payload (T) {			
Next payload	‘00001011’B	Next payload is RAND	
TS Type	‘00000011’B	NTP-UTC-32 (3)	
TS Value	3710502000	A randomly chose value = Corresponds to 31/07/2017, 17:00:00. The time of issue represented by the number of seconds since 0h on 1 January 1900 with respect to the Coordinated Universal Time (UTC)	
}			
RAND Payload {			
Next payload	‘00001110’B	Next payload is IDRi	
RAND len	‘00010000’B	16 Bytes RAND	
RAND	128-bit random number		
}			
IDRi payload {			
Next payload	‘00001110’B	Next payload is IDRi	
ID Role	1	Initiator (IDRi)	
ID Type	0	URI	
ID len	Length of ID Data		
ID data	px_MCPTT_User_A_ID	MCPTT ID associated with the initiating user	
}			
IDRr payload {			
Next payload	‘00001110’B	Next payload is IDRkmsi	
ID Role	2	Responder (IDRr)	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
ID Type	0		
ID len	Length of ID Data		
ID data	px_MCPTT_User_B_ID	MCPTT ID associated to the receiving user	
}			
IDRkmsi payload {			
Next payload	'00001110'B	Next payload is IDRkmsr	
ID Role	6	Initiator's KMS (IDRkmsi)	
ID Type	0		
ID len	Length of ID Data		
ID data	px_MCPTT_KMS	the URI of the MCPTT KMS used by the initiating user	
}			
IDRkmsr payload {			
Next payload	'00001010'B	Next payload is Security Properties	
ID Role	7	Responder's KMS (IDRkmsr)	
ID Type	0		
ID len	Length of ID Data		
ID data	px_MCPTT_KMS	the URI of the MCPTT KMS used by the terminating user	
}			
Security Properties payload {		When not included the content specified below is assumed	
Next payload	'00011010'B	Next payload is SAKKE (26)	
Policy no	'00000001'B	Random nr	
Prot type	0	SRTP	
Policy param length			
Policy param {			
{			
Type	0	Encryption Algorithm	
length			
value	6	AES-GCM	
}			
{			
Type	1	Session encryption key length	
length			
value	16	16 octets	
}			
{			
Type	4	Session salt key length	
length			
value	12	12 octets	
}			
{			
Type	5	SRTP PRF	
length			
value	0	AES-CM	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
}			
{			
Type	6	Key derivation rate	
length			
value	0	No session key refresh.	
}			
{			
Type	20	AEAD authentication tag length	
length			
value	16	16 octets	
}			
}			
}			
SAKKE payload {			
Next payload	'00000100'B	Next payload is SIGN	
SAKKE params {	1	RFC 6509 [23], Appendix A	
n	128		
p	997ABB1F 0A563FDA 65C61198 DAD0657A 416C0CE1 9CB48261 BE9AE358 B3E01A2E F40AAB27 E2FC0F1B 228730D5 31A59CB0 E791B39F F7C88A19 356D27F4 A666A6D0 E26C6487 326B4CD4 512AC5CD 65681CE1 B6AFF4A8 31852A82 A7CF3C52 1C3C09AA 9F94D6AF 56971F1F FCE3E823 89857DB0 80C5DF10 AC7ACE87 666D807A FEA85FEB		
q	265EAEC7 C2958FF6 99718466 36B4195E 905B0338 672D2098 6FA6B8D6 2CF8068B BD02AAC9 F8BF03C6 C8A1CC35 4C69672C 39E46CE7 FDF22286 4D5B49FD 2999A9B4 389B1921 CC9AD335 144AB173 595A0738 6DABFD2A 0C614AA0 A9F3CF14 870F026A A7E535AB D5A5C7C7 FF38FA08 E2615F6C 203177C4 2B1EB3A1 D99B601E BFAA17FB		

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
Px	53FC09EE 332C29AD 0A799005 3ED9B52A 2B1A2FD6 0AEC69C6 98B2F204 B6FF7CBF B5EDB6C0 F6CE2308 AB10DB90 30B09E10 43D5F22C DB9DFA55 718BD9E7 406CE890 9760AF76 5DD5BCCB 337C8654 8B72F2E1 A702C339 7A60DE74 A7C1514D BA66910D D5CFB4CC 80728D87 EE9163A5 B63F73EC 80EC46C4 967E0979 880DC8AB EAE63895		
Py	0A824906 3F6009F1 F9F1F053 3634A135 D3E82016 02990696 3D778D82 1E141178 F5EA69F4 654EC2B9 E7F7F5E5 F0DE55F6 6B598CCF 9A140B2E 416CFF0C A9E032B9 70DAE117 AD547C6C CAD696B5 B7652FE0 AC6F1E80 164AA989 492D979F C5A4D5F2 13515AD7 E9CB99A9 80BDAD5A D5BB4636 ADB9B570 6A67DCDE 75573FD7 1BEF16D7		
g	66FC2A43 2B6EA392 148F1586 7D623068 C6A87BD1 FB94C41E 27FABE65 8E015A87 371E9474 4C96FEDA 449AE956 3F8BC446 CBFDA85D 5D00EF57 7072DA8F 541721BE EE0FAED1 828EAB90 B99DFB01 38C78433 55DF0460 B4A9FD74 B4F1A32B CAFA1FFA D682C033 A7942BCC E3720F20 B9B7B040 3C8CAE87 B7A0042A CDE0FAB3 6461EA46		
Hash	SHA-256	(defined in [FIPS180-3]	
}			
ID Scheme	'URI Scheme'		
SAKKE data length		16 bits	
SAKKE data	encapsulate the PCK to the UID generated from the MCPTT ID of the terminating user		
}			
SIGN (ECCSI) payload {			
Next payload	‘00000000’B	This is the last payload	
S type	2	ECCSI signature	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
S data	encapsulate the PCK to the UID generated from the MCPTT ID of the terminating user		
}			

Table 5.5.9.1-3: MIKEY-SAKKE I_MESSAGE (GMK distribution)

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
MIKEY Common Header {	Any		
version	'00000001'B		
Data Type	'00011010'B	SAKKE msg (26)	
Next payload	'00000101'B	Next payload is timestamp	
V	'0'B		
PRF func	'0000001'B	PRF-HMAC-SHA-256	
CSB ID	GUK-ID	Group User Key Identifier Derived from GMK-ID and User Salt	
#CS	'00000001'B	the number of crypto sessions in the CS ID map info.	
CS ID map type	2	GENERIC-ID	
CS ID map Info {			
CS ID	'00000011'B	the CS ID of the crypto session 8 bits	
Prot type	0	SRTP the security protocol to be used for the crypto session	
S	1	the ROC and SEQ fields are provided	
#P	1	the number of security policies provided for the crypto session	
Ps {		lists the policies for the crypto session	
Policy_no_1	'00000001'B	a policy_no that corresponds to the policy_no of a SP payload	
}			
Session Data Length		16 bits the length of Session Data (in bytes). For the Prot type SRTP, Session Data MAY be omitted in the initial message (length = 0), but it MUST be provided in the response message.	
Session Data {		session data for the crypto session	
SSRC		specifies the SSRC that MUST be used for the crypto session	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
ROC		current/initial rollover counter. If the session has not started, this field is set to '0'	
SEQ		current/initial sequence number	
}			
SPI Length		SPI MAY be omitted in the initial message (length = 0), but it MUST be provided in the response message	
SPI		the SPI (or MKI) corresponding to the session key to (initially) be used for the crypto session. Other keys can be used.	
}			
}			
Timestamp Payload (T) {			
Next payload	‘00001011’B	Next payload is RAND	
TS Type	‘00000011’B	NTP-UTC-32 (3)	
TS Value	3710502000	A randomly chose value = Corresponds to 31/07/2017, 17:00:00. The time of issue represented by the number of seconds since 0h on 1 January 1900 with respect to the Coordinated Universal Time (UTC)	
}			
RAND Payload {			
Next payload	‘00001110’B	Next payload is IDRi	
RAND len	‘00010000’B	16 Bytes RAND	
RAND	128-bit random number		
}			
IDRi payload {			
Next payload	‘00001110’B	Next payload is IDRr	
ID Role	1	Initiator (IDRi)	
ID Type	1	URI	
ID len	Length of ID Data		

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
ID data	px_MCPTT_GMS	MCPTT identifier associated with the group management server	
}			
IDRr payload {			
Next payload	'00001110'B	Next payload is IDRkmsi	
ID Role	2	Responder (IDRr)	
ID Type	0		
ID len	Length of ID Data		
ID data	px_MCPTT_User_A_ID	MCPTT ID associated to the group management client	
}			
IDRkmsi payload {			
Next payload	'00001110'B	Next payload is IDRkmsr	
ID Role	6	Initiator's KMS (IDRkmsi)	
ID Type	0		
ID len	Length of ID Data		
ID data	px_MCPTT_KMS	the URI of the MCPTT KMS used by the group management server	
}			
IDRkmsr payload {			
Next payload	'00001010'B	Next payload is SP (Security Properties)	
ID Role	7	Responder's KMS (IDRkmsr)	
ID Type	0		
ID len	Length of ID Data		
ID data	px_MCPTT_KMS	the URI of the MCPTT KMS used by the MCPTT user	
}			
Security Properties payload {		When not included the content specified below is assumed	
Next payload	'00011010'B	Next payload is SAKKE (26)	
Policy no	'00000001'B	Random nr	
Prot type	0	SRTP	
Policy param length			
Policy param {			
{			
Type	0	Encryption Algorithm	
length			
value	6	AES-GCM	
}			

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
{			
Type	1	Session encryption key length	
length			
value	16	16 octets	
}			
{			
Type	4	Session salt key length	
length			
value	12	12 octets	
}			
{			
Type	5	SRTP PRF	
length			
value	0	AES-CM	
}			
{			
Type	6	Key derivation rate	
length			
value	0	No session key refresh.	
}			
{			
Type	20	AEAD authentication tag length	
length			
value	16	16 octets	
}			
}			
}			
SAKKE payload {			
Next payload	‘00010101’B	Next payload is General Extension	
SAKKE params {	1	RFC 6509 [23], Appendix A	
n	128		
p	997ABB1F 0A563FDA 65C61198 DAD0657A 416C0CE1 9CB48261 BE9AE358 B3E01A2E F40AAB27 E2FC0F1B 228730D5 31A59CB0 E791B39F F7C88A19 356D27F4 A666A6D0 E26C6487 326B4CD4 512AC5CD 65681CE1 B6AFF4A8 31852A82 A7CF3C52 1C3C09AA 9F94D6AF 56971F1F FCE3E823 89857DB0 80C5DF10 AC7ACE87 666D807A FEA85FEB		

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
q	265EAEC7 C2958FF6 99718466 36B4195E 905B0338 672D2098 6FA6B8D6 2CF8068B BD02AAC9 F8BF03C6 C8A1CC35 4C69672C 39E46CE7 FDF22286 4D5B49FD 2999A9B4 389B1921 CC9AD335 144AB173 595A0738 6DABFD2A 0C614AA0 A9F3CF14 870F026A A7E535AB D5A5C7C7 FF38FA08 E2615F6C 203177C4 2B1EB3A1 D99B601E BFAA17FB		
Px	53FC09EE 332C29AD 0A799005 3ED9B52A 2B1A2FD6 0AEC69C6 98B2F204 B6FF7CBF B5EDB6C0 F6CE2308 AB10DB90 30B09E10 43D5F22C DB9DFA55 718BD9E7 406CE890 9760AF76 5DD5BCCB 337C8654 8B72F2E1 A702C339 7A60DE74 A7C1514D BA66910D D5CFB4CC 80728D87 EE9163A5 B63F73EC 80EC46C4 967E0979 880DC8AB EAE63895		
Py	0A824906 3F6009F1 F9F1F053 3634A135 D3E82016 02990696 3D778D82 1E141178 F5EA69F4 654EC2B9 E7F7F5E5 F0DE55F6 6B598CCF 9A140B2E 416CFF0C A9E032B9 70DAE117 AD547C6C CAD696B5 B7652FE0 AC6F1E80 164AA989 492D979F C5A4D5F2 13515AD7 E9CB99A9 80BDAD5A D5BB4636 ADB9B570 6A67DCDE 75573FD7 1BEF16D7		

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
g	66FC2A43 2B6EA392 148F1586 7D623068 C6A87BD1 FB94C41E 27FABE65 8E015A87 371E9474 4C96FEDA 449AE956 3F8BC446 CBFDA85D 5D00EF57 7072DA8F 541721BE EE0FAED1 828EAB90 B99DFB01 38C78433 55DF0460 B4A9FD74 B4F1A32B CAFA1FFA D682C033 A7942BCC E3720F20 B9B7B040 3C8CAE87 B7A0042A CDE0FAB3 6461EA46		
Hash	SHA-256	(defined in [FIPS180-3]	
}			
ID Scheme	'3GPP MCX hashed UID'		
SAKKE data length		16 bits length of SAKKE data (in bytes)	
SAKKE data	encapsulate the GMK to the UID generated from the MCPTT ID of the group management client		
}			
General Extension Payload {			
Next payload	‘00000100’B	Next payload is SIGN	
Type	'3GPP key parameters'	See 33.179 [15] clause E.6	
..Length		The length in bytes of the Data field	
Data {		See 33.179 [15] clause E.6	
Key Type	‘00000000’B	GMK	
Status	'1'	Not-revoked	
Activation Time	0	The time in UTC at which the associated GMK is to be made active for transmission in seconds since midnight UTC of January 1, 1970 (not counting leap seconds). It shall be 5 octets in length. A value of 0 shall imply the activation time is the timestamp of the received MIKEY I_MESSAGE	

Derivation path: RFC 6509 [23], RFC 6043 [25], RFC 3830 [24]			
Field	**Value/remark**	**Comment**	**Condition**
Expiry Time		The 'Expiry time' element shall define the time in UTC at which the associated key shall no longer be used in seconds since midnight UTC of January 1, 1970 (not counting leap seconds). It shall be 5 octets in length. A value of 0 shall imply the key shall not expire.	
Text			
Group IDs {			
Number of Group IDs	'1'		
Group ID	px_MCPTT_Group_A_ID	The ID for the group associated with the key.	
}			
}			
}			
SIGN (ECCSI) payload {			
Next payload	‘00000000’B	This is the last payload	
S type	2	ECCSI signature	
S data		The signature shall use the UID generated from the identifier associated with the group management server	
}			

5.5.10 Common MCPTT test USIM parameters

5.5.10.1 General

The format and coding of elementary files of the USIM are defined in 3GPP TS 31.102 [73]. Those of the ISIM are defined in 3GPP TS 31.101 [79] and 3GPP TS 31.103 [80].

The present clause defines default MCPTT relevant parameters for programming the elementary files of the test USIM when running conformance test cases defined in 3GPP TS 36.579-2 [2].

For requirements to the test USIM/ISIM needed for the E-UTRA/EPC and MCPTT off-network ProSe operation see 3GPP TS 36.508 [6], subclause 4.9.

5.5.10.2 Default settings for the Elementary Files (EFs)

EF_{UST} (USIM Service Table)

Services	Discription	Activated	Version
Service n°109	MCPTT	Yes	
NOTE: Only the relevant MCPTT related services indicated.			

EF_{MST} (MCPTT Service Table)

This file shall be present. This EF indicates the coding of the MCPTT management objects and which MCPTT services are available.

Coding of the MCPTT management objects = '00' (XML format).

Services	Discription	Activated	Version
Service n°1:	UE configuration data	Yes	
Service n°2:	User configuration data	Yes	
Service n°3:	Group configuration data	Yes	
Service n°4:	Service configuration data	Yes	

EF_{MCPTT_CONFIG} (MCPTT configuration data)

This file shall be present.

Encoded in XML format (as specified in the MCPTT Service Table).

MCPTT configuration data objects	Tag Values	Condition
MCPTT UE configuration data	'80'	Shall be present. The content of the MCPTT UE configuration data object shall be as specified in Table 5.5.8.2-1.
MCPTT User configuration data	'81'	Shall be present. The content of the MCPTT User configuration data object shall be as specified in Table 5.5.8.3-1.
MCPTT Group configuration data	'82'	Shall be present. The content of the MCPTT Group configuration data object shall be as specified in Table 5.5.7.1-1.
MCPTT Service configuration data	'83'	Shall be present. The content of the MCPTT Server configuration data object shall be as specified in Table 5.5.8.4-1.

5.6 Reference configurations

5.6.1 General

The Reference configuration requirements provided in subclause 5.6 specify configuration values that are expected to be pre-configured in the UE before a test is started. The exception to this requirement are tests which verify the communication exchange which allows a MCPTT device to be enabled for the provision of MCPTT cervices e.g. test case 5.1 in TS 36.579-2 [2].

5.6.2 Key material for provisioning of End-to-end communication security

For any end-point to use or access end-to-end secure communications, it needs to be provisioned with keying material associated to its identity by the KMS as specified in 3GPP TS 33.179 [15]. To avoid dynamic allocation of key material before each test case is run, the following keying information needs to be preconfigured in the UE. For convenience, the

information is provided in the form of an XML which can be provided/pre-configured in the UE e.g. by a Key Management Server (KMS) as specified in 3GPP TS 33.179 [15].

```
<?xml version="1.0" encoding="UTF-8"?>
<SignedKmsResponse xmlns= "TOBEDEFINED" xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ds = "http://www.w3.org/2000/09/xmldsig#" xmlns:se = "TOBEDEFINED"
    xsi:schemaLocation = "TOBEDEFINED SE_KmsInterface_XMLSchema.xsd" Id = "xmldoc">
<KmsResponse xmlns= "TOBEDEFINED"  Version = "1.0.0">
  <KmsUri>kms.example.org</KmsUri>
  <UserUri>user@example.org</UserUri>
  <Time>2014-01-26T10:07:14</Time>
  <KmsId>KMSProvider12345</KmsId>
  <ClientReqUrl>http://kms.example.org/keymanagement/identity/v1/keyprov</ClientReqUrl>
  <KmsMessage>
    <KmsKeyProv Version = "1.0.0" xsi:type = "se:KmsKeyProvTkType">
      <KmsKeySet Version = "1.1.0">
        <KmsUri>kms.example.org</KmsUri>
        <CertUri>cert1.kms.example.org</CertUri>
        <Issuer>www.example.org</Issuer>
        <UserUri>user@example.org</UserUri>
        <UserID>0123456789ABCDEF0123456789ABCDEF</UserID>
        <ValidFrom>2017-07-31T17:00:00</ValidFrom>
        <ValidTo>2018-07-31T16:59:59</ValidTo>
        <KeyPeriodNo>3710502000</KeyPeriodNo>
        <Revoked>false</Revoked>
        <UserDecryptKey xsi:type = "se:EncKeyContentType">
          <EncryptedKey xmlns = "http://www.w3.org/2001/04/xmlenc#">
            <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes256"/>
            <ds:KeyInfo>
              <ds:KeyName>tk.12.user@example.org</KeyName>
            </ds:KeyInfo>
            <CipherData>
              <CipherValue>DEADBEEF</CipherValue>
            </CipherData>
          </EncryptedKey>
        </UserDecryptKey>
        <UserSigningKeySSK xsi:type = "se:EncKeyContentType">
          <EncryptedKey xmlns = "http://www.w3.org/2001/04/xmlenc#">
            <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes256"/>
            <ds:KeyInfo>
              <ds:KeyName>tk.12.user@example.org</KeyName>
            </ds:KeyInfo>
            <CipherData>
              <CipherValue>DEADBEEF</CipherValue>
            </CipherData>
        </EncryptedKey>
        </UserSigningKeySSK>
        <UserPubTokenPVT xsi:type = "se:EncKeyContentType">
          <EncryptedKey xmlns = "http://www.w3.org/2001/04/xmlenc#">
            <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes256"/>
            <ds:KeyInfo>
              <ds:KeyName>tk.12.user@example.org</KeyName>
            </ds:KeyInfo>
            <CipherData>
              <CipherValue>DEADBEEF</CipherValue>
            </CipherData>
          </EncryptedKey>
        </UserPubTokenPVT>
      </KmsKeySet>
      <NewTransportKey xmlns= "TOBEDEFINED">
            <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#"
Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey">
              <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes256"/>
              <ds:KeyInfo>
                <ds:KeyName>tk.12.user@example.org</KeyName>
              </ds:KeyInfo>
              <CipherData>
                <CipherValue>DEADBEEF</CipherValue>
              </CipherData>
              <CarriedKeyName>tk.13.user@example.org</CarriedKeyName>
            </EncryptedKey>
          </NewTransportKey>
    </KmsKeyProv>
  </KmsMessage>
</KmsResponse>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

```
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-sha256">
        <HMACOutputLength>128</HMACOutputLength>
      </SignatureMethod>
      <Reference URI="#xmldoc">
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <DigestValue>nnnn</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>DEADBEEF</SignatureValue>
    <KeyInfo>
      <KeyName>tk.12.user@example.org</KeyName>
    </KeyInfo>
  </Signature>
</SignedKmsResponse>
```

5.6.3 XML schema for MCPTT location information

```
From TS 24.379 clause F.3.2:
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:mcpttloc="urn:3gpp:ns:mcpttLocationInfo:1.0"
targetNamespace="urn:3gpp:ns:mcpttLocationInfo:1.0" elementFormDefault="qualified"
attributeFormDefault="unqualified"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

    <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"/>

    <xs:element name="location-info" id="loc">
        <xs:annotation>
            <xs:documentation>Root element, contains all information related to location
configuration, location request and location reporting for the MCPTT service</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:choice>
                <xs:element name="Configuration" type="mcpttloc:tConfigurationType"/>
                <xs:element name="Request" type="mcpttloc:tRequestType"/>
                <xs:element name="Report" type="mcpttloc:tReportType"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
            </xs:choice>
            <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="tConfigurationType">
        <xs:sequence>
            <xs:element name="NonEmergencyLocationInformation"
type="mcpttloc:tRequestedLocationType" minOccurs="0"/>
            <xs:element name="EmergencyLocationInformation" type="mcpttloc:tRequestedLocationType"
minOccurs="0"/>
            <xs:element name="TriggeringCriteria" type="mcpttloc:TriggeringCriteriaType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="ConfigScope">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Full"/>
                    <xs:enumeration value="Update"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tRequestType">
        <xs:complexContent>
            <xs:extension base="mcpttloc:tEmptyType">
                <xs:attribute name="RequestId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="tReportType">
        <xs:sequence>
            <xs:element name="TriggerId" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="CurrentLocation" type="mcpttloc:tCurrentLocationType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
```

```
        </xs:sequence>
        <xs:attribute name="ReportID" type="xs:string" use="optional"/>
        <xs:attribute name="ReportType" use="required">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Emergency"/>
                    <xs:enumeration value="NonEmergency"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:attribute>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="TriggeringCriteriaType">
        <xs:sequence>
            <xs:element name="CellChange" type="mcpttloc:tCellChange" minOccurs="0"/>
            <xs:element name="TrackingAreaChange" type="mcpttloc:tTrackingAreaChangeType"
minOccurs="0"/>
            <xs:element name="PlmnChange" type="mcpttloc:tPlmnChangeType" minOccurs="0"/>
            <xs:element name="MbmsSaChange" type="mcpttloc:tMbmsSaChangeType" minOccurs="0"/>
            <xs:element name="MbsfnAreaChange" type="mcpttloc:tMbsfnAreaChangeType" minOccurs="0"/>
            <xs:element name="PeriodicReport" type="mcpttloc:tIntegerAttributeType" minOccurs="0"/>
            <xs:element name="TravelledDistance" type="mcpttloc:tIntegerAttributeType"
minOccurs="0"/>
            <xs:element name="McpttSignallingEvent" type="mcpttloc:tSignallingEventType"
minOccurs="0"/>
            <xs:element name="GeographicalAreaChange" type="mcpttloc:tGeographicalAreaChange"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tCellChange">
        <xs:sequence>
            <xs:element name="AnyCellChange" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificCell" type="mcpttloc:tSpecificCellType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="ExitSpecificCell" type="mcpttloc:tSpecificCellType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEmptyType"/>
    <xs:simpleType name="tEcgi">
        <xs:restriction base="xs:string">
            <xs:pattern value="\d{3}\d{3}[0-1]{28}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tSpecificCellType">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tEcgi">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tEmptyTypeAttribute">
        <xs:complexContent>
            <xs:extension base="mcpttloc:tEmptyType">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="tTrackingAreaChangeType">
        <xs:sequence>
            <xs:element name="AnyTrackingAreaChange" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="EnterSpecificTrackingArea" type="mcpttloc:tTrackingAreaIdentity"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="ExitSpecificTrackingArea" type="mcpttloc:tTrackingAreaIdentity"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tTrackingAreaIdentityFormat">
        <xs:restriction base="xs:string">
```

```
            <xs:pattern value="\d{3}\d{3}[0-1]{16}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tTrackingAreaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tTrackingAreaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tPlmnChangeType">
        <xs:sequence>
            <xs:element name="AnyPlmnChange" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificPlmn" type="mcpttloc:tPlmnIdentity" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="ExitSpecificPlmn" type="mcpttloc:tPlmnIdentity" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tPlmnIdentityFormat">
        <xs:restriction base="xs:string">
            <xs:pattern value="\d{3}\d{3}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tPlmnIdentity">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tPlmnIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tMbmsSaChangeType">
        <xs:sequence>
            <xs:element name="AnyMbmsSaChange" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificMbmsSa" type="mcpttloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:element name="ExitSpecificMbmsSa" type="mcpttloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tMbmsSaIdentityFormat">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="65535"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tMbmsSaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tMbmsSaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tMbsfnAreaChangeType">
        <xs:sequence>
            <xs:element name="EnterSpecificMbsfnArea" type="mcpttloc:tMbsfnAreaIdentity"
minOccurs="0"/>
            <xs:element name="ExitSpecificMbsfnArea" type="mcpttloc:tMbsfnAreaIdentity"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:simpleType name="tMbsfnAreaIdentityFormat">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="255"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tMbsfnAreaIdentity">
        <xs:simpleContent>
            <xs:extension base="mcpttloc:tMbsfnAreaIdentityFormat">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
```

```
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tIntegerAttributeType">
        <xs:simpleContent>
            <xs:extension base="xs:integer">
                <xs:attribute name="TriggerId" type="xs:string" use="required"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
    <xs:complexType name="tTravelledDistanceType">
        <xs:sequence>
            <xs:element name="TravelledDistance" type="xs:positiveInteger"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tSignallingEventType">
        <xs:sequence>
            <xs:element name="InitialLogOn" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="GroupCallNonEmergency" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="PrivateCallNonEmergency" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="LocationConfigurationReceived" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type=" mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEmergencyEventType">
        <xs:sequence>
            <xs:element name="GroupCallEmergency" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="GroupCallImminentPeril" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="PrivateCallEmergency" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:element name="InitiateEmergencyAlert" type="mcpttloc:tEmptyTypeAttribute"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tRequestedLocationType">
        <xs:sequence>
            <xs:element name="ServingEcgi" type="mcpttloc:tEmptyType" minOccurs="0"/>
            <xs:element name="NeighbouringEcgi" type="mcpttloc:tEmptyType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="MbmsSaId" type="mcpttloc:tEmptyType" minOccurs="0"/>
            <xs:element name="MbsfnArea" type="mcpttloc:tEmptyType" minOccurs="0"/>
            <xs:element name="GeographicalCordinate" type="mcpttloc:tEmptyType" minOccurs="0"/>
            <xs:element name="minimumIntervalLength" type="xs:positiveInteger"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tCurrentLocationType">
        <xs:sequence>
            <xs:element name="CurrentServingEcgi" type="mcpttloc:tLocationType" minOccurs="0"/>
            <xs:element name="NeighbouringEcgi" type="mcpttloc:tLocationType" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="MbmsSaId" type="mcpttloc:tLocationType" minOccurs="0"/>
            <xs:element name="MbsfnArea" type="mcpttloc:tLocationType" minOccurs="0"/>
            <xs:element name="CurrentCoordinate" type="mcpttloc:tPointCoordinate" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:simpleType name="protectionType">
        <xs:restriction base="xs:string">
```

```
            <xs:enumeration value="Normal"/>
            <xs:enumeration value="Encrypted"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="tLocationType">
        <xs:choice minOccurs="1" maxOccurs="1">
            <xs:element name="Ecgi" type="mcpttloc:tEcgi" minOccurs="0"/>
            <xs:element name="SaId" type="mcpttloc:tMbmsSaIdentity" minOccurs="0"/>
            <xs:element name="MbsfnAreaId" type="mcpttloc:tMbsfnAreaIdentity" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:choice>
        <xs:attribute name="type" type="protectionType"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tGeographicalAreaChange">
        <xs:sequence>
            <xs:element name="AnyAreaChange" type="mcpttloc:tEmptyTypeAttribute" minOccurs="0"/>
            <xs:element name="EnterSpecificAreaType" type="mcpttloc:tSpecificAreaType"
minOccurs="0"/>
            <xs:element name="ExitSpecificAreaType" type="mcpttloc:tSpecificAreaType"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tSpecificAreaType">
        <xs:sequence>
            <xs:element name="GeographicalArea" type="mcpttloc:tGeographicalAreaDef"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="TriggerId" type="xs:string" use="required"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tPointCoordinate">
        <xs:sequence>
            <xs:element name="longitude" type="mcpttloc:tCoordinateType"/>
            <xs:element name="latitude" type="mcpttloc:tCoordinateType"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="tCoordinateType">
        <xs:choice minOccurs="1" maxOccurs="1">
            <xs:element name="threebytes" type="mcpttloc:tThreeByteType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:choice>
        <xs:attribute name="type" type="protectionType"/>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>

    <xs:simpleType name="tThreeByteType">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="16777215"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tGeographicalAreaDef">
        <xs:sequence>
            <xs:element name="PolygonArea" type="mcpttloc:tPolygonAreaType" minOccurs="0"/>
            <xs:element name="EllipsoidArcArea" type="mcpttloc:tEllipsoidArcType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tPolygonAreaType">
        <xs:sequence>
            <xs:element name="Corner" type="mcpttloc:tPointCoordinate" minOccurs="3"
maxOccurs="15"/>
```

```
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="tEllipsoidArcType">
        <xs:sequence>
            <xs:element name="Center" type="mcpttloc:tPointCoordinate"/>
            <xs:element name="Radius" type="xs:nonNegativeInteger"/>
            <xs:element name="OffsetAngle" type="xs:unsignedByte"/>
            <xs:element name="IncludedAngle" type="xs:unsignedByte"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="anyExt" type="mcpttloc:anyExtType" minOccurs="0"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:complexType>
    <xs:complexType name="anyExtType">
        <xs:sequence>
            <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-02	R5#74	R5-171298	-	-	-	Introduction of TS 36.579-1.	0.0.1
2017-05	R5#75	R5-172100	-	-	-	Introduction of default message content for some media control messages, some generic procedures from R5-172078 Default MCPTT media plane control messages R5-172079 Generic MCPTT procedures	0.0.2
2017-06	RAN5#75	-	-	-	-	lifted to v0.1.0 because of technical contents	0.1.0
2017-08	RAN5#76	R5-173766	-	-	-	Implemented approved: R5-173702 'Various updates of MCPTT TS 36579-1' R5-173703 'Update of MCPTT generic procedures' R5-173704 'New Generic procedures ProSe and MCPTT' R5-173705 'Update default media plane control messages' R5-173706 'Update of MCPTT Default MCPTT call control Off-network messages' R5-173707 'Update of MCPTT MIKEY-SAKKE I.MESSAGE' R5-173766 'Update of TS 36.579-1 to version 0.2.0' R5-174599 'SIP message defaults for 36.579-1' R5-174600 'MCPTT Off-Network Group Call Signaling Message Defaults'	0.2.0
2017-12	RAN5#77	R5-176835	-	-	-	Implemented approved: R5-177000 "Update of SIP Message Defaults for MCPTT" R5-176345 "Update of Specific SIP messages in Generic procedures" R5-177001 "Update of Generic procedures for SIP registration" R5-176347 "New Generic Procedure for ProSe group calls Announcing-Discoveree procedure for group member discovery" R5-176348 "New Generic Procedure for ProSe group calls Monitoring/Discoverer procedure for group member discovery" R5-177002 "Update with UE Configuration Defaults" - References updates	0.3.0
2017-12	RAN#78	RP-172182	-	-	-	Draft version for information purposes to the RAN Plneary	1.0.0
2018-03	RAN5#78	R5-180684	-	-	-	Implemented approved: R5-180534 "Update of Section 5.5.2 and 5.5.3 for TS 36.579-1" R5-180535 "Update of Section 5.5.5 for TS 36.579-1" R5-180536 "Update of Section 5.5.6 for TS 36.579-1" R5-181241 "Update of Section 5.5.9 TS 36.579-1" R5-180633 "Update of Default HTTP message and other information elements" R5-180634 "Update of Default MCPTT configuration management messages" R5-180635 "New Generic procedures for MCPTT Authorization/Configuration and Key Generation" R5-18063 "New Generic procedures for MCPTT communication in E-UTRA / Change of cells" R5-180637 "Generic Test Procedure for MCPTT communication over MBMS" R5-180638 "Various updates to 36579-1"	1.1.0
2018-03	RAN#79	RP-180126	-	-	-	Draft version for approval to move the spec under revision control to the RAN Plenary	2.0.0
2018-03	RAN#79	-	-	-	-	Editorial changes and promoted to v13.0.0	13.0.0
2018-06	RAN#80	R5-182418	0001	-	F	Addition and correction of GNSS information	13.1.0
2018-06	RAN#80	R5-182419	0002	-	F	Editorial correction of typos and incorrect references	13.1.0
2018-06	RAN#80	R5-182430	0003	-	F	Editorial Update of 36.579-2 for style H6	13.1.0
2018-06	RAN#80	R5-182431	0004	-	F	Update of TC 5.1 for MCPTT APN	13.1.0
2018-06	RAN#80	R5-182432	0005	-	F	Updates of Location information messages in 36.579-2	13.1.0
2018-06	RAN#80	R5-182489	0008	-	F	Update of MCPTT TC 6.1.1.1	13.1.0
2018-06	RAN#80	R5-182510	0009	-	F	Correction to MCPTT TC of 6.1.1.8, 6.1.1.11, 6.1.2.5 and 6.1.2.7	13.1.0
2018-06	RAN#80	R5-183167	0006	1	F	Updates of TC 6.3.1	13.1.0
2018-06	RAN#80	R5-183168	0007	1	F	Updates of TC 6.3.2	13.1.0
2018-09	RAN#81	R5-185084	0009	-	F	Update to TLS setup	13.2.0
2018-09	RAN#81	R5-185122	0007	1	F	Corrections to MCPTT Authorization	13.2.0
2018-09	RAN#81	R5-184685	0008	-	F	Update of default message contents for new Rel-14 TCs for Private Call Call-Back and Ambient listening call	14.0.0
2018-12	RAN#82	R5-186878	0010	-	F	Correction to Generic Test Procedure for MCPTT pre-established session establishment CO	14.1.0
2018-12	RAN#82	R5-186879	0011	-	F	Editorial update of the default SDP and Resource-list Messages	14.1.0
2018-12	RAN#82	R5-186880	0012	-	F	Update of default MCPTT media plane control messages and other information elements to reflect latest Rel-13 core specs	14.1.0
2018-12	RAN#82	R5-186881	0013	-	F	Update of XML schema for MCPTT location information to reflect latest Rel-13 core specs	14.1.0
2018-12	RAN#82	R5-187709	0014	1	F	Corrections to clause 5.5.9 of 36.579-1	14.1.0
2018-12	RAN#82	R5-187710	0015	1	F	Corrections to clause 5.5.7.1 of 36.579-1	14.1.0
2018-12	RAN#82	R5-187711	0016	1	F	Update for Resource-lists in 36.579-1	14.1.0

2018-12	RAN#82	R5-187712	0017	1	F	Correction to Table 5.5.1-1 in 36.579-1	14.1.0
2018-12	RAN#82	R5-187713	0018	1	F	Correction to Table 5.5.4.10.1-1 in 36.579-1	14.1.0
2018-12	RAN#82	R5-187714	0019	1	F	Correction to Table 5.5.4.2-1 in 36.579-1	14.1.0
2018-12	RAN#82	R5-187715	0020	1	F	Correction to SIP NOTIFY message in 36.579-1	14.1.0
2018-12	RAN#82	R5-187716	0021	1	F	Correction to SIP SUBSCRIBE message in 36.579-1	14.1.0
2018-12	RAN#82	R5-187717	0022	1	F	Update of Generic Test 5.3.2 in 36.579-1	14.1.0
2019-03	RAN#83	R5-191210	0023	-	F	Correction of default contents in SIP INVITE from the UE	14.2.0
2019-03	RAN#83	R5-191902	0024	-	F	Update to MCPTT floor control default messages	14.2.0
2019-03	RAN#83	R5-192155	0025	-	F	Update 36.579-1 Section 4.2 and 4.3	14.2.0
2019-03	RAN#83	R5-192156	0026	-	F	Update 36.579-1 Delete subclauses inside the present spec	14.2.0
2019-03	RAN#83	R5-192157	0027	-	F	Update 36.579-1 Blue text removal	14.2.0
2019-06	RAN#84	R5-194001	0028	-	F	Correction of default contents in the SIP INVITE from the UE	14.3.0
2019-06	RAN#84	R5-194665	0030	-	F	Typo for MCPTT in 36.579-1	14.3.0
2019-06	RAN#84	R5-195216	0029	1	F	Update of UE registration procedure for location info configuration	14.3.0
2019-06	RAN#84	R5-195217	0031	1	F	References and derivation path updates for SIP messages	14.3.0

History

Document history		
V14.0.0	October 2018	Publication
V14.1.0	December 2018	Publication
V14.2.0	May 2019	Publication
V14.3.0	July 2019	Publication