ETSI TS 123 179 V13.0.0 (2016-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
Functional architecture and information flows to support mission critical communication services;
(3GPP TS 23.179 version 13.0.0 Release 13)

Reference
RTS/TSGS-0623179vd00

Keywords
LTE,UMTS

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

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

Intellectual Property Rights

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

Foreword

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This document specifies the functional architecture, procedures and information flows needed to support the mission critical push to talk (MCPTT) service including the common services core architecture for identity management, group management, and configuration management required to support the MCPTT voice service. Support for both MCPTT group calls and MCPTT private calls operating in on-network and off-network modes of operation is specified.

The corresponding service requirements are defined in 3GPP TS 22.179 [2].

The present document is applicable primarily to MCPTT voice service using E-UTRAN access based on the EPC architecture defined in 3GPP TS 23.401 [9]. Certain MCPTT functions such as dispatch and administrative functions could also be supported via non-3GPP access networks but no additional functionality is specified to support non-3GPP access.

The MCPTT service requires preferential handling compared to normal telecommunication services e.g. in support of police or fire brigade including the handling of prioritised MCPTT calls for emergency and imminent threats.

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

In the present document, MCPTT calls between MCPTT users on different MCPTT systems are considered, however, for roaming only EPC-level roaming and IMS-level roaming are considered i.e. partner MCPTT system based roaming (also known as "migration") is out of scope.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

[3] 3GPP TS 23.002: "Network Architecture".

[4] 3GPP TS 23.203: "Policy and charging control architecture".

[5] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[6] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 2".

[7] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[8] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[9] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[10] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".

[11] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[12] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE_LTE); MB2 Reference Point; Stage 3".

[13] 3GPP TS 33.179: "Security of Mission Critical Push-To-Talk (MCPTT)".

[14] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

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

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].

Automatic commencement mode: A mode in which the initiation of the private call does not require any action on the part of the receiving MCPTT user.

Group affiliation: A mechanism by which an MCPTT user's interest in one or more MCPTT groups is determined.

Group call: A mechanism by which an MCPTT user can make a one-to-many MCPTT transmission to other users that are members of MCPTT group(s).

Group de-affiliation: A mechanism by which an MCPTT user's interest in one or more MCPTT groups is removed.

Group home MCPTT system: The MCPTT system where the MCPTT group is defined.

Group host MCPTT server: The MCPTT server within an MCPTT system which provides centralised support for MCPTT services of an MCPTT group defined in a group home MCPTT system.

Manual commencement mode: A mode in which the initiation of the private call requires the receiving MCPTT user to perform some action to accept or reject the call setup.

On-network MCPTT service: The collection of functions and capabilities required to provide MCPTT via EPS bearers using E-UTRAN to provide the last hop radio bearers.

UE-to-network relay MCPTT service: The collection of functions and capabilities required to provide MCPTT via a ProSe UE-to-network relay using ProSe direct communication paths to provide the last hop radio bearer(s).

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

Dispatcher
Floor control
MCPTT administrator
MCPTT service
MCPTT system
MCPTT UE
MCPTT user
MCPTT User Profile
Mission Critical Organization
Mission Critical Push To Talk
Off-network MCPTT service
Partner MCPTT system
Primary MCPTT system
Private call

For the purposes of the present document, the following terms and definitions given in IETF RFC 5245 [15] apply:

Candidate
Candidate pair

3.2 Symbols

For the purposes of the present document, the following symbols given in 3GPP TS 22.179 [2] apply:

B1
B2
N2
N3
N4
N5
N6
N7
N10
N11

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].

APN	Access Point Name
ARP	Allocation and Retention Priority
BM-SC	Broadcast Multicast Service Centre
CSCF	Call Server Control Function
DL	Downlink
DPF	Direct Provisioning Function
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
ECGI	E-UTRAN Cell Global Identifier
EPC	Evolved Packet Core
EPS	Evolved Packet System
GBR	Guaranteed Bit Rate
GCS AS	Group Communication Service Application Server
GCSE_LTE	Group Communication Service Enabler over LTE
GRUU	Globally Routable User agent URI
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
I-CSCF	Interrogating CSCF
ICE	Interactive Connectivity Establishment
IM CN	IP Multimedia Core Network
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia PUblic identity
IMS	IP Multimedia Subsystem
MBMS	Multimedia Broadcast and Multicast Service
MBSFN	Multimedia Broadcast multicast service Single Frequency Network
MC	Mission Critical
MC ID	Mission Critical user identity
MCPTT	Mission Critical Push To Talk
MCPTT AS	MCPTT Application Server
MCPTT group ID	MCPTT group identity
MCPTT ID	MCPTT user identity
NAT	Network Address Translation
P-CSCF	Proxy CSCF
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
PLMN	Public Land Mobile Network
ProSe	Proximity-based Services
PSI	Public Service Identity

PTT	Push To Talk
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
S-CSCF	Serving CSCF
SAI	Service Area Identifier
SDF	Service Data Flow
SIP	Session Initiated Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TMGI	Temporary Mobile Group Identity
UM	Unacknowledged Mode
USB	Universal Serial Bus
URI	Uniform Resource Identifier
WLAN	Wireless Local Area Network

4 Introduction

The MCPTT service supports communication between several users (i.e. group call), where each user has the ability to gain access to the permission to talk in an arbitrated manner. The MCPTT service also supports private calls between two users.

The MCPTT architecture utilises aspects of the IMS architecture defined in 3GPP TS 23.228 [5], the Proximity-based Services (ProSe) architecture defined in 3GPP TS 23.303 [8], the Group Communication System Enablers for LTE (GCSE_LTE) architecture defined in 3GPP TS 23.468 [10] and the PS-PS access transfer procedures defined in 3GPP TS 23.237 [6] to enable support of the MCPTT service.

The MCPTT UE primarily obtains access to the MCPTT service via E-UTRAN, using the EPS architecture defined in 3GPP TS 23.401 [9]. Certain MCPTT functions such as dispatch and administrative functions can be supported using either MCPTT UEs in E-UTRAN or using MCPTT UEs via non-3GPP access networks.

NOTE: Dispatch consoles and devices used by MCPTT service administrators are considered MCPTT UEs in the MCPTT architecture.

MCPTT UEs that use non-3GPP access can only support a subset of the functionality specified in this specification that is supported by the non-3GPP access network.

5 Assumptions and architectural requirements

5.1 Assumptions

5.1.1 Service continuity

Service continuity feature shall only be supported between on-network MCPTT service and UE-to-network relay MCPTT service, for both group calls and private calls.

The MCPTT UE, prior to going out of E-UTRAN coverage, should attempt to make use of a ProSe UE-to-network relay in order to support the service continuity.

5.2 Architectural requirements

5.2.1 General architectural requirements

General MCPTT architectural requirements include:

a) To develop economies of scale, it will be useful if PLMN operators can reuse the MCPTT architecture for non-public safety customers that require similar functionality. These PLMN operators may want to integrate many components of the MCPTT solution with their existing network architecture.

   Hence a functional decomposition of MCPTT into a small number of distinct logical functions is required.

b) The architecture should enable an application plane and signalling control plane split for the provision of the MCPTT service.

c) To enable parts of the MCPTT solution to be reused for other applications, the architecture should enable the group management functions (e.g. admission control; linking of groups; etc) to be implemented on a separate node from the main PTT functions (e.g. 'call' setup/termination; allocation of TMGI to UE; floor control; etc).

d) There is a need to promptly form (and release) groups of users that span multiple public safety network administrations. To enable this, the architecture should provide the relevant interfaces between public safety networks.

5.2.2 Roaming requirements

The MCPTT application can provide MCPTT service to users in various PLMNs. Roaming is supported using EPC-level roaming or IMS-level roaming.

5.2.3 Media routing requirements

The voice media flow for a private call shall be routed according to one of the following two options:

a) Option 1:

   1) Through the primary MCPTT system if both users in the call belong to the same organisation; or

   2) Through the primary MCPTT system of both users, if the users in the call do not belong to the same organisation.

b) Option 2: The voice media flow may be routed locally, under the control of the primary MCPTT system, through an entity allowing the duplication of the media flow to the primary MCPTT system of each user.

The voice media flow for a group call shall be routed to the group home MCPTT system.

The routing of media flow shall be end-to-end from transmitter to receiver(s), except for the MCPTT control function.

5.2.4 Requirements for user identity management

To allow for confidentiality of user identities in various cases of business relationship as defined in clause 6, the MCPTT application may provide public user identities to the MCPTT UE, to be used by MCPTT UE for MCPTT services.

The MCPTT application providing the identities may be located in the primary MCPTT system or in a partner MCPTT system under the control of the primary MCPTT system.

This provision is subject to preliminary authentication of the MCPTT user.

5.2.5 Group affiliation and de-affiliation

Group affiliation can be achieved through the following two methods:

a) Explicit affiliation: An MCPTT user provides interest in one or many MCPTT groups using the MCPTT UE. An MCPTT authorized user may remotely modify another MCPTT user's affiliation to an MCPTT group.

b) Implicit affiliation: MCPTT user's affiliations to MCPTT groups are determined through configurations and policies at the MCPTT UE or MCPTT service and performed implicitly by the associated MCPTT UE or MCPTT service.

NOTE: Group affiliation is not the same as group membership; however, an MCPTT user is a member of a group prior to becoming an affiliated member of that group.

The following functionality shall be enabled by the MCPTT service for the MCPTT users affiliated to the MCPTT groups:

- MCPTT users receive notifications for group call setup and invitation for their affiliated group(s).
- MCPTT users can select amongst their affiliated group a selected MCPTT group for media transmission. Thus, allowing the MCPTT user to initiate a new group call or transmit in an existing group call.
- MCPTT users receive media and events from their affiliated group(s).

Group de-affiliation indicates that the MCPTT user is no longer affiliated to that MCPTT group, and therefore is not able to perform any actions that are associated with an affiliated member e.g. receive media, notifications, etc. De-affiliation can occur either through MCPTT user's explicit request, or implicitly (e.g. changed as the result of another action, such as the user logging off).

5.2.6 MCPTT call requirements

5.2.6.1 General

The on-network MCPTT service shall support the use of pre-established sessions.

5.2.6.2 Group call requirements

The MCPTT service shall support the chat group (restricted) call model for MCPTT group call.

The MCPTT service shall support the pre-arranged group call model for MCPTT group call.

5.2.7 GCS AS requirements for the MCPTT service

Point to multipoint broadcast offered by the LTE MBMS technology is well suited to group communications, which form a major part of the public safety related communications. MCPTT relies on this capability in the form of MCPTT MBMS, in addition to unicast communications and off-network communications (ProSe).

The MCPTT on-network architecture, is based in part on 3GPP TS 23.468 [10] with the MCPTT AS assuming the function of the GCS AS and can be represented (in a simplified diagram) as shown in figure 5.2.7-1:

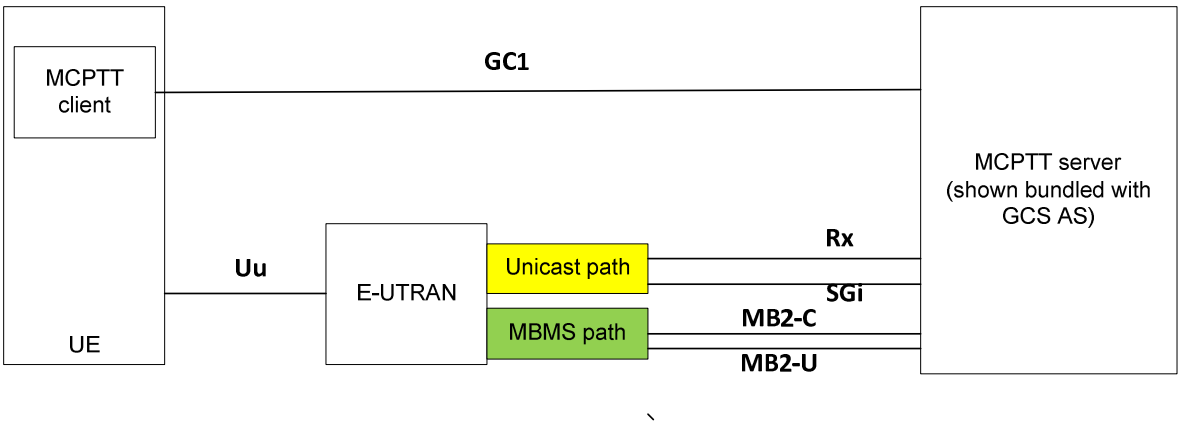

Figure 5.2.7-1: MCPTT on-network architecture showing MBMS

The MCPTT server is shown being bundled with the GCS AS within the same network entity. It is illustrated this way for simplicity of the diagram.

MCPTT media content is transmitted via LTE bearers, which are communication pipes with one end in the MCPTT server and the other end in the MCPTT UE. The uplink bearers are always allocated as unicast, but the downlink bearers can be allocated as unicast or as MBMS bearers, or both.

An MBMS bearer (both network and radio part) is uniquely identified via a TMGI or via a combination of a TMGI and a flow identifier (see 3GPP TS 23.246 [7]). The MCPTT server is capable, via the MB2 interface, to request the creation of MBMS bearers and associate a unique TMGI or a combination of a TMGI and a flow identifier (see 3GPP TS 23.468 [10]). The MCPTT server may determine the MBMS broadcast area based on the cell identities of the affiliated group members received over MCPTT-1.

5.2.8 UE-to-network relay MCPTT service requirements

To support the requirement that a public safety ProSe UE-to-network relay shall be able to restrict the relayed group communication on a per group basis, the MCPTT service should be able to provide a means for an MCPTT administrator to configure a ProSe UE-to-network relay with a list of allowed MCPTT groups. For each allowed MCPTT group, a unique associated relay service code should be allocated and it may be provided to the relay UE from MCPTT application server or DPF.

NOTE: According to the PLMN operator's configuration, one relay service code can map to one or multiple MCPTT group(s).

5.2.9 Bearer management

5.2.9.1 General

The MCPTT system shall use an MCPTT system specific APN.

5.2.9.2 EPS bearer considerations for SIP signalling and HTTP

If the PDN connection established during the initial attach by the UE is to an APN other than the MCPTT specific APN, then prior to user authentication, the UE shall establish another PDN connection to the MCPTT specific APN. PDN connection establishment can also be caused by a SIP registration request for MCPTT.

The QCI value of 69 (as specified in 3GPP TS 23.203 [4]) shall be used for the EPS bearer that transports SIP-1 reference point messaging. The QCI value 8 (as specified in 3GPP TS 23.203 [4]) or better shall be used for the EPS bearer that transports HTTP-1 reference point messaging.

5.2.9.3 EPS unicast bearer considerations for MCPTT

For an MCPTT call session request, resources shall be requested utilising interaction with dynamic PCC. The MCPTT system shall request resources over Rx to a PCRF. The dedicated bearer for voice and MCPTT-4 reference point messaging shall utilise the QCI value of 65 (as specified in 3GPP TS 23.203 [4]). The request of resources over Rx shall include an application identifier for MCPTT in order for the PCRF to evaluate the correct QCI.

The UE is required to support at minimum one UM bearer which is used for MCPTT voice (see annex B in 3GPP TS 36.331 [14]).

Depending on operator policy:

- the MCPTT system may be able to request modification of the priority (ARP) of an existing bearer without the need to initiate a new dedicated GBR bearer; or

- the EPS bearers for MCPTT call may enable pre-emption of lower priority EPS bearers due to maximum number of UM bearer has been reached in favour of MCPTT initiated EPS bearer. In this case the EPS bearer used for MCPTT call shall have higher priority level (ARP) than the UM bearer(s) used for other application(s). Furthermore bearers for non MCPTT application must be pre-emptable. As a consequence, the EPS bearer for MCPTT call overrides one of the existing EPS bearers when the maximum number of bearers is established for other applications.

The EPS bearer for MCPTT emergency call shall have highest priority level among MCPTT call types. The EPS bearer for MCPTT imminent peril call shall have higher priority level than one for MCPTT call.

To ensure that the MCPTT service always has access to a dedicated bearer for MCPTT media, a pre-established session may be setup that includes a request for resources at the first MCPTT group affiliation.

This means that the PCC may multiplex MCPTT media streams from multiple concurrent MCPTT calls into one EPS bearer on one shared network priority regardless of MCPTT call priority.

NOTE 1: A single UM bearer is used to multiplex the media streams from multiple concurrent MCPTT calls.

NOTE 2: The sharing of a single GBR bearer for voice means that different QCI and/or ARP values are not possible for different voice media streams.

5.2.9.4 MBMS bearer management

When operating in systems that support MBMS functionality, the MCPTT service shall be able to provide downlink MBMS delivery of MCPTT media.

When operating in systems that support MBMS functionality, the MCPTT service shall be able to provide downlink MBMS delivery of floor control messages targeted towards multiple MCPTT clients at the same time (specifically floor idle and floor taken).

MCPTT UEs shall be able to receive the traffic delivered via MBMS, regardless of whether or not they have any unicast radio bearers available.

When switching MCPTT service between different downlink bearers, the MCPTT UE shall preserve the reception context in order to eliminate or reduce to a minimum any interruption of service.

The MCPTT service shall enable an MCPTT UE which has just entered an area of media delivery via MBMS bearers to immediately start receiving the media of an ongoing MCPTT group call.

The MCPTT server shall not map MCPTT group calls to MBMS bearers that cannot provide the QoS required by the group.

An MCPTT UE should be able to support eight MBSFN areas simultaneously on the same RF carrier.

5.2.10 MCPTT system interconnect requirements

The architecture for interconnect between MCPTT systems is specified, allowing the affiliation of MCPTT users from an MCPTT system with MCPTT groups defined in another MCPTT system. When both MCPTT systems are served by different networks, interconnect of signalling and media is achieved using the interfaces defined for interconnect between PLMNs.

6 Involved business relationships

Based on the information in subclause 5.2.1 and subclause 5.2.2, figure 6-1 shows the business relationships that exist and that are needed to support a single MCPTT user.

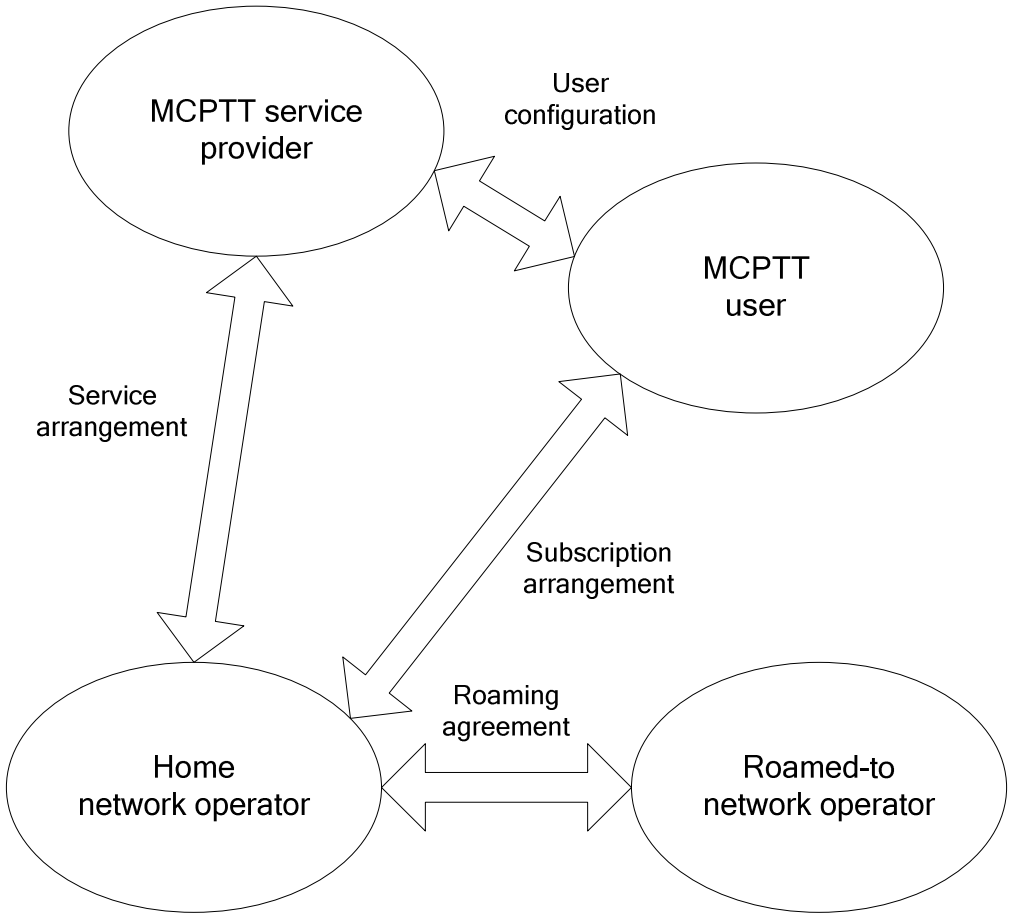

Figure 6-1: Business relationships for MCPTT

The MCPTT service provider and the home PLMN operator could be part of the same organisation, in which case the business relationship between the two is internal to a single organisation.

Multiple MCPTT service providers can be supported by the same home PLMN operator.

Where mutual aid operates between MCPTT service providers, figure 6-2 shows the required additional relationship. An MCPTT user can only affiliate to groups of the partner MCPTT service provider:

- if such a service provider agreement exists; or
- subject to authorisation for a specific group membership from the partner MCPTT service provider.

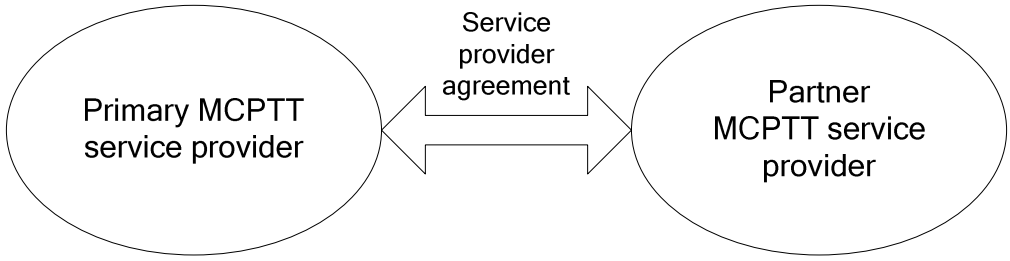

Figure 6-2: Additional business relationships for mutual aid

The primary and partner MCPTT service providers do not need to be served by the same home SIP core operator in order to support mutual communication and mutual aid when interconnection between the SIP cores is available.

An example of the usage of these business relationships is elaborated for two users, one resident on its primary MCPTT service provider and one providing mutual aid within the same group.

User A is a user on MCPTT X in group M. The relationships are as follows:

a) user A has user configuration established with MCPTT X and forms part of group M;

b) user A has a subscription arrangement with PLMN operator R; and

c) MCPTT X has a service arrangement with PLMN operator R.

User B is a user on MCPTT Y and joins group M as part of a mutual aid:

a) user B has user configuration established with MCPTT Y and forms part of its own set of groups relating to MCPTT Y;

b) user B has a subscription arrangement with PLMN operator S;

c) MCPTT Y has a service arrangement with PLMN operator S;

d) MCPTT Y has a service provider agreement with MCPTT X that allows user B to participate within group M; and

e) PLMN operator S has a roaming agreement with PLMN operator R allowing user B to roam to PLMN operator R.

NOTE: There is no requirement that the PLMN operator that user B roams to is the same PLMN operator that MCPTT X has a service arrangement with. It does however need to support MCPTT capabilities, and provides service in the same geographic area as used by MCPTT X.

7 Functional model

7.1 General

The functional model for the support of MCPTT is defined as a series of planes to allow for the breakdown of the architectural description.

Further, each plane is expected to operate in an independent manner, providing services to the connected planes as and when requested by the connected plane, and requesting services from other planes as required.

As a consequence of this each plane should manage on its own behalf:

a) use of identities. Each plane is therefore responsible for the privacy of that plane's own identities; and

b) security for that plane. This does not preclude a plane requesting security services from another plane, but that is a decision made within the plane, as to whether to use offered security services or mechanisms within the plane itself.

NOTE: Terminology such as client and server are not meant to imply specific physical implementation of a functional entity.

7.2 Description of the planes

The following planes are identified:

a) application plane. The application plane provides all of the services (e.g. call control, floor control) required by the user together with the necessary functions to support media control and transfer. It uses the services of the signalling control plane to support those requirements. The application plane also provides for the conferencing of media, transcoding of media, and provision of tones and announcements; and

b) signalling control plane. The signalling control plane provides the necessary signalling support to establish the association of users involved in an MCPTT call or other type of call and other services. The signalling control plane also offers access to and control of services applicable to calls. The signalling control plane uses the services of the bearer plane.

Bearers supporting these planes are defined for LTE within 3GPP TS 23.401 [9]. The resource control that is needed to support these planes is defined within 3GPP TS 23.203 [4]. The application plane also relies on the use of multicast bearers established via procedures defined in 3GPP TS 23 468 [10] and 3GPP TS 23.246 [7].

7.3 Functional model description

7.3.1 On-network functional model

Figure 7.3.1-1 shows the functional model for the application plane.

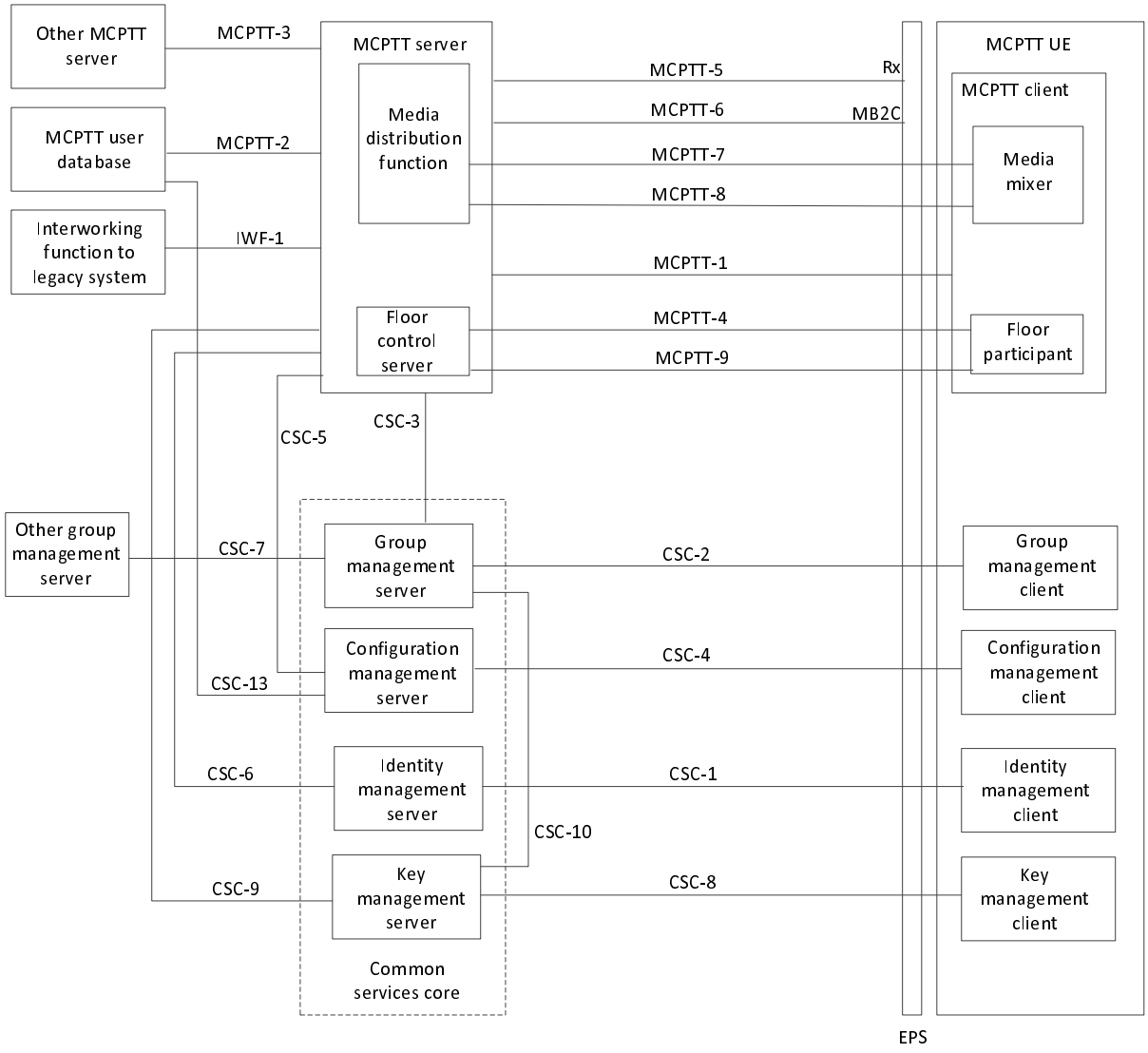

Figure 7.3.1-1: Functional model for application plane

In the model shown in figure 7.3.1-1, the following apply:

- The MCPTT AS is an instantiation of a GCS AS in accordance with 3GPP TS 23.468 [10].
- The MCPTT user database may be combined with an HSS in some deployment scenarios (e.g. when the MCPTT service provider and the PLMN operator are part of the same trust domain).
- MCPTT-9 carries multicast floor control signalling between the floor control server of the MCPTT server and the floor participant of the MCPTT UE.
- MCPTT-4 carries unicast floor control signalling between the floor control server of the MCPTT server and the floor participant of the MCPTT UE.

- MCPTT-7 carries unicast media between the media distribution function of the MCPTT server and the media mixer of the MCPTT UE.
- MCPTT-8 carries multicast media from the media distribution function of the MCPTT server to the media mixer of the MCPTT UE.

Figure 7.3.1-2 shows the functional model for the signalling control plane.

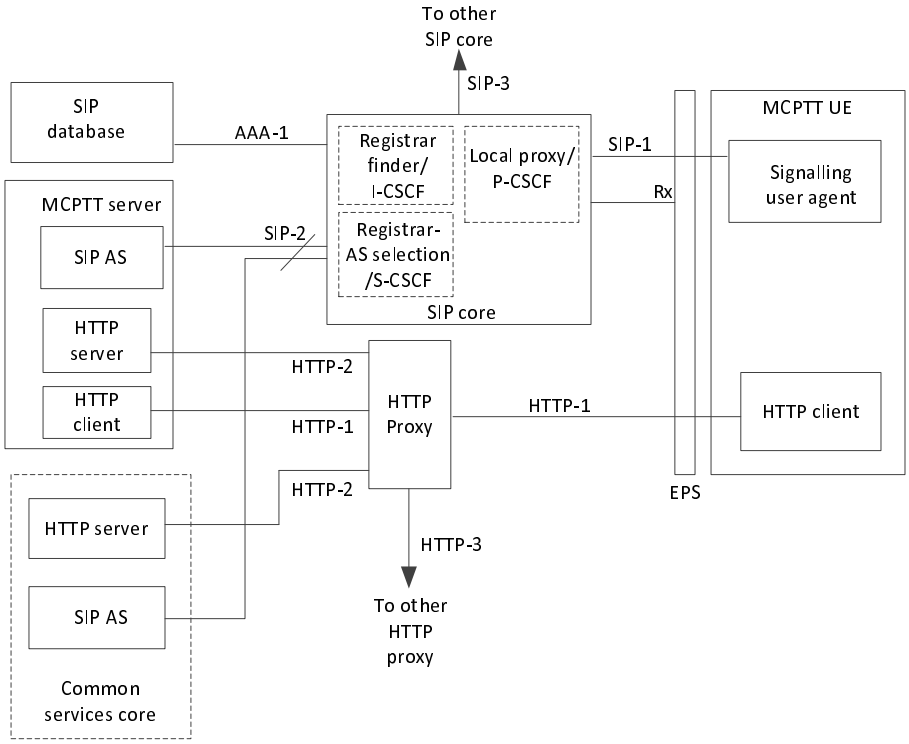

Figure 7.3.1-2: Functional model for signalling control plane

Figure 7.3.1-3 shows the relationships between the reference points of the application plane and the signalling plane.

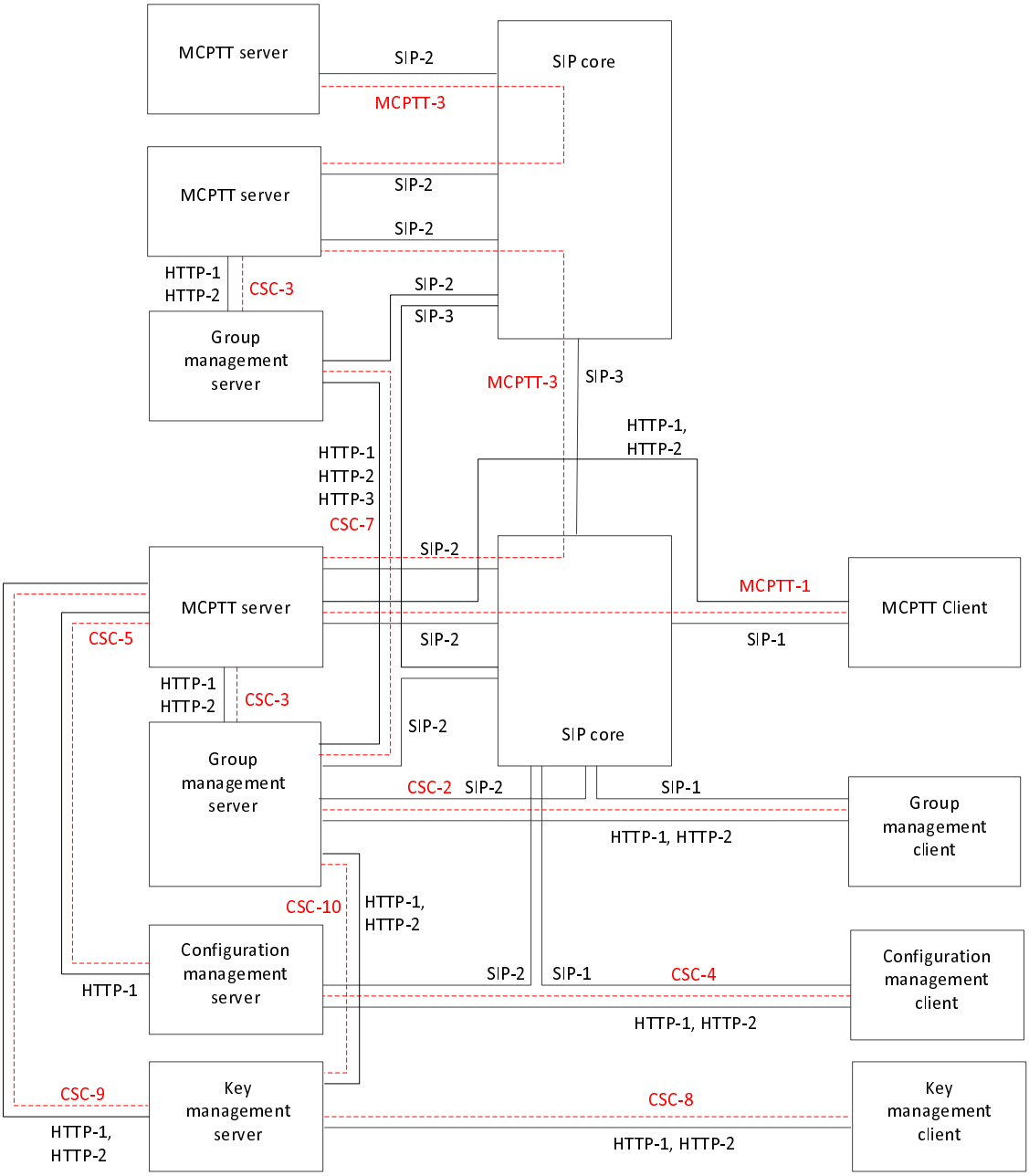

Figure 7.3.1-3: Relationships between reference points of application and signalling control planes

NOTE 1: Application plane reference point CSC-7 makes use of SIP-2 reference point when the group management servers are connected by a single SIP core. Where they are joined by more than one SIP core, CSC-7 also makes use of the SIP-3 reference point.

NOTE 2: For simplicity, the HTTP proxy, which provides the interconnection between HTTP-1, HTTP-2 and HTTP-3 reference points, is not shown in figure 7.3.1-3.

7.3.2 Off-network functional model

Figure 7.3.2-1 shows the functional model for off-network operation.

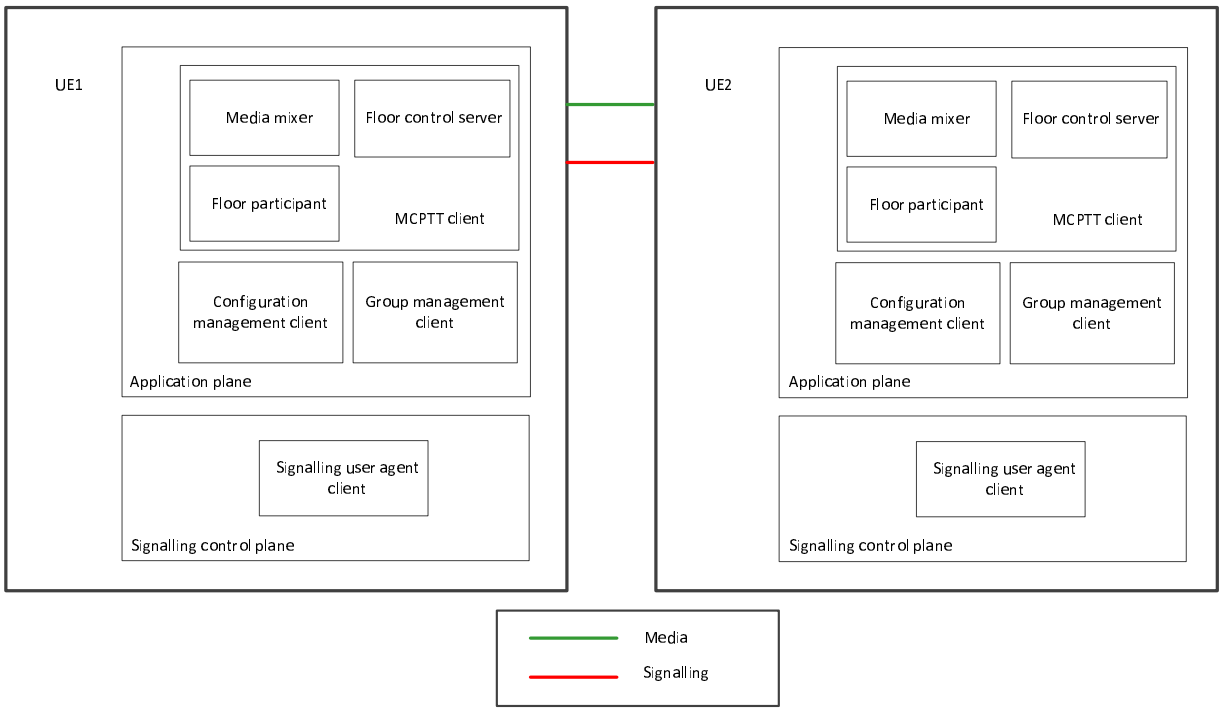

Figure 7.3.2-1: Functional model for off-network operation

7.4 Functional entities description

7.4.1 General

Each subclause is a description of a functional entity and does not imply a physical entity.

7.4.2 Application plane

7.4.2.1 General

Entities within the application plane provide application control, media control and distribution functions.

7.4.2.2 Common services core

7.4.2.2.1 Configuration management client

The configuration management client functional entity acts as the application user agent for configuration related transactions. The configuration management client interacts with the configuration management server and provides and receives configuration data.

The configuration management client functional entity is supported by the signalling user agent and HTTP client functional entities of the signalling control plane.

7.4.2.2.2 Configuration management server

The configuration management server is a functional entity used to configure the MCPTT application with non-group management MCPTT service related information and configure data on the configuration management client. The configuration management server manages MCPTT service configuration supported within the MCPTT service provider.

The configuration management server functional entity is supported by the SIP AS and HTTP server functional entities of the signalling control plane.

7.4.2.2.3 Group management client

The group management client functional entity acts as the application user agent for management of MCPTT groups. It interacts with the group management server.

The group management client functional entity is supported by the signalling user agent and HTTP client functional entities of the signalling control plane.

7.4.2.2.4 Group management server

The group management server functional entity provides for management of groups supported within the MCPTT service provider.

The group management server functional entity is supported by the SIP AS and HTTP server functional entities of the signalling control plane.

All the group management clients supporting users belonging to a single group are required to use the same group management server for that group. A group management client supporting a user involved in multiple groups can have relationships with multiple group management servers.

The group management server manages media policy information for use by the UE for media mixing.

The group management server manages group call policy information for use by the UE for both on-network and off-network group call control.

7.4.2.2.5 Identity management client

This functional entity acts as the application user agent for MC ID transactions. It interacts with the identity management server.

7.4.2.2.6 Identity management server

The identity management server is a functional entity that is capable of authenticating the MC ID. It contains the knowledge and means to do authentication by verifying the credentials supplied by the user.

The identity management server functional entity may reside in the same domain as the user's MCPTT server.

7.4.2.2.7 Key management client

This functional entity acts as the application user agent for key management functions. It interacts with the key management server.

The functionality of the key management client is specified in 3GPP TS 33.179 [13].

7.4.2.2.8 Key management server

The key management server is a functional entity that stores and provides security related information (e.g. encryption keys) to the key management client, group management server and MCPTT server to achieve the security goals of confidentiality and integrity of media and signalling.

The functionality of the key management server is specified in 3GPP TS 33.179 [13].

7.4.2.3 MCPTT application service

7.4.2.3.1 MCPTT client

The MCPTT client functional entity acts as the user agent for all MCPTT application transactions. The client reports the information of where the client is currently located.

7.4.2.3.2 MCPTT server

The MCPTT server functional entity provides centralised support for MCPTT services.

All the MCPTT clients supporting users belonging to a single group are required to use the same MCPTT server for that group. An MCPTT client supporting a user involved in multiple groups can have relationships with multiple MCPTT servers.

NOTE: Possible requirements for handling multiple distinct media on different MCPTT servers are not covered in this version of the document.

The MCPTT server functional entity represents a specific instantiation of the GCS AS described in 3GPP TS 23.468 [10] to control multicast and unicast operations for group communications.

The MCPTT server functional entity is supported by the SIP AS, HTTP client and HTTP server functional entities of the signalling control plane.

By assuming the role of a GCS AS, the MCPTT server functional entity is responsible for:

- keeping track of MCPTT UE location with respect to multicast service availability;
- requesting the allocation of multicast resources utilizing the media distribution function;
- announcing the association of multicast resources to calls to MCPTT UEs;
- determining for each MCPTT UE involved in a given call whether to use unicast or multicast transport;
- announcing the assignment of multicast transport for specific calls to MCPTT UEs; and
- informing the media distribution function of the media streams requiring support for a given call.

The MCPTT server shall support the controlling role and the participating role. The MCPTT server may perform the controlling role for private calls and group calls. The MCPTT server performing the controlling role for a private call or group call may also perform a participating role for the same private call or group call. For each private call and group call, there shall be only one MCPTT server assuming the controlling role, while one or more MCPTT servers in participating role may be involved.

The MCPTT server performing the controlling role is responsible for:

- call control (e.g. policy enforcement for participation in the MCPTT group calls) towards all the MCPTT users of the group call and private call;
- managing floor control entity in a group call and private call; and
- managing media handling entity in call i.e. conferencing, transcoding.

The MCPTT server performing the participating role is responsible for:

- call control (e.g. authorization for participation in the MCPTT group calls) to its MCPTT users for group call and private call;
- group affiliation support for MCPTT user, including enforcement of maximum N2 number of simultaneous group affiliations by a user;
- relaying the call control and floor control messages between the MCPTT client and the MCPTT server performing the controlling role; and
- media handling in call for its MCPTT users, i.e. transcoding, recording, lawful interception for both unicast and multicast media.

For group regrouping involving multiple groups from primary and partner MCPTT systems,

- the group host MCPTT server of the temporary group performs the controlling role and is responsible for the centralized floor control, and for arbitration according to the temporary group or user policies (e.g., priority);

- the group host MCPTT server of the constituent MCPTT group is responsible for providing call invitations to their group members, and for filtering between constituent group members" floor control requests according to the constituent group or user policies (e.g., priority); and

- the MCPTT server responsible for the constituent MCPTT group members performs the participating role.

7.4.2.3.3 Floor participant

The floor participant functional entity is responsible for floor requests. This functional entity is located in the UE for both on-network and off-network operations.

7.4.2.3.4 Floor control server

This functional entity provides support for centralised floor control for on-network and distributed floor control for off-network operation. It may provide arbitration between floor control requests between different users, grant the floor in response to successful requests, and provide queuing in cases of contention. For on-network operation, this functional entity is located with the MCPTT server. For off-network operation, this functional entity is located in the UE.

7.4.2.3.5 Media distribution function

The media distribution function is responsible for the distribution of media to call participants. By means of information provided by the MCPTT server (e.g. IP addresses, transport layer ports, etc), it will provide the following functionality:

- provide for the reception of uplink MCPTT UE media transmission by means of the MCPTT-7 reference point;

- replicate the media as needed for distribution to those participants using unicast transport;

- distribute downlink media to MCPTT UEs by IP unicast transmission to those participants utilizing unicast transport by means of the MCPTT-7 reference point;

- distribute downlink media to MCPTT UEs using multicast downlink transport of media for the call by means of the MCPTT-8 reference point; and

- provide a media mixing function where multiple media streams are combined into a single media stream for transmission to the MCPTT UE.

NOTE 1: If media mixing function occurs within the media distribution function, it operates independently of the media mixer in the UE.

NOTE 2: A media mixing function within the media distribution function is not possible where the media is end to end encrypted.

7.4.2.3.6 Media mixer

This functional entity exists on the UE and provides support for combining multiple media streams into one media stream through the enforcement of media policy information.

7.4.2.3.7 MCPTT user database

This functional entity contains information of all user configuration information associated with an MCPTT ID that is held by the MCPTT service provider at the application plane. User configuration information is determined by the MCPTT service provider.

7.4.3 Signalling control plane

7.4.3.1 SIP entities

7.4.3.1.1 Signalling user agent

This functional entity acts as the SIP user agent (both client and server) for all SIP transactions

7.4.3.1.2 SIP AS

The SIP AS functional entity supports the following functions on behalf of the MCPTT service:

- influencing and impacts the SIP session; and
- supporting event subscription and notification.

NOTE: In the IM CN subsystem, this is provided by the Application Server as defined in 3GPP TS 23.002 [3].

7.4.3.1.3 SIP core

7.4.3.1.3.1 General

The SIP core contains a number of sub-entities responsible for registration, service selection and routing in the signalling control plane.

The SIP core shall be either:

1. compliant with 3GPP TS 23.228 [5], i.e. the SIP core is a 3GPP IP multimedia core network subsystem; or
2. a SIP core, which internally need not comply with the architecture of 3GPP TS 23.228 [5], but with the reference points that are defined in subclause 7.5.3 (if exposed), compliant to the reference points defined in 3GPP TS 23.002 [3].

The data related to the functions of the SIP core, e.g. for data for application service selection, the identity of the serving registrar or authentication related information may be provided by the PLMN operator responsible for the bearer plane. In this case, the SIP database that is the source of the data may be part of the HSS. Alternatively, this data may be provided by the MCPTT service provider. In this case, the source of the data may be the MCPTT service provider"s SIP database.

Editor's note: Access restrictions to data between different trust domains and related security aspects are currently under consideration by SA3.

7.4.3.1.3.2 Local inbound / outbound proxy

The local inbound / outbound proxy functional entity acts as both an inbound proxy and an outbound proxy for all SIP transactions. This functional entity can provide the following functions:

- NAT traversal;
- Resource control;
- Route/forward requests and responses to the user agents;
- SIP signalling security; and
- Depending on the PLMN operator policy, discovery and address resolution, including E.164 numbers.

NOTE: In the IM CN subsystem, this functional entity is provided by the P-CSCF as defined in 3GPP TS 23.228 [5].

7.4.3.1.3.3 Registrar finder

The registrar finder functional entity is responsible for:

a) Identifying the serving registrar / application service selection functional entity. The serving registrar / application service selection functional entity is identified using information provided either by the PLMN operator's own SIP database or the MCPTT service provider's SIP database, and optionally using the PLMN operator's internal information e.g. network topology, registrar availability.

   1) Registrar finder and registrar in the MCPTT service provider domain: registrar finder in the MCPTT service provider's domain uses the information from the MCPTT service provider"s SIP database to identify the serving registrar in the MCPTT service provider domain.

2) Registrar finder and registrar in the PLMN operator domain: registrar finder uses information from PLMN operator's SIP database to identify the serving registrar in the PLMN operator domain.

3) Registrar finder in PLMN operator domain and registrar in MCPTT service provider domain: registrar finder uses information from the MCPTT service provider"s SIP database to identify the serving registrar in the MCPTT service provider domain.

NOTE 1: The need for the registrar finder is deployment specific e.g. a deployment that has only one registrar does not need the registrar finder and the related SIP database information.

b) Providing discovery and address resolution, including E.164 numbers.

NOTE 2: In the IM CN subsystem, this is provided by the I-CSCF as defined in 3GPP TS 23.228 [5].

7.4.3.1.3.4 Registrar / application service selection

The registrar / application service selection functional entity provides the following functions:

- Registrar function (with integral provision of a location server) and also acts as an inbound proxy (with access to the integral location server), and outbound proxy for all SIP transactions where application service selection is required. It registers the user and maintains the association of the location and identity of the user in a location service. It provides notifications of the registration states.

- Supports authentication for identities provided within SIP signalling. Both the registrar (with integral location server) and authentication functions are supported by access either to the public network's own SIP database or the MCPTT service provider's SIP database.

- Can provide the application service selection for all SIP transactions, possibly based on application service selection information stored by either the public network's own SIP database or the MCPTT service provider's SIP database.

- Performs SIP signalling security.

NOTE: In the IM CN subsystem, this is provided by the S-CSCF as defined in 3GPP TS 23.228 [5].

7.4.3.2 SIP database

7.4.3.2.1 General

The SIP database contains information concerning the SIP subscriptions and corresponding identity and authentication information required by the SIP core, and such information as application service selection.

In deployment scenarios where the PLMN operator provides the SIP core, this database is provided by the HSS.

In deployment scenarios where the MCPTT service provider provides the SIP core, the SIP database may be provided by the MCPTT service provider.

Access to the data residing in the SIP database is restricted to the SIP core entities that are specifically serving the subscriber/user whose data are stored, i.e. registrars and registrar finders can access SIP databases only when they are part of the same trust domain for the data being provided.

NOTE: The SIP database can be in a different network than the registrar finder since the trust domain for the criteria for registrar selection can be different than the trust domain for the signalling plane user identities.

The SIP database is responsible for storing the following user related information:

- signalling plane user identities: Numbering and addressing information;

- signalling plane security information: SIP core access control information for authentication and authorization;

- MCPTT UE Location information at inter-system level: the SIP database supports the user registration, and stores inter-system location information, etc.; and

- signalling plane subscription profile (including initial filter criteria).

The SIP database also generates signalling plane security information for mutual authentication, communication integrity check and ciphering.

Based on this information, the SIP database is also responsible to support the call control and session management entities of the SIP core.

The SIP database consists of the following functionalities:

- support for control functions of the SIP core such as the Registrar and Registrar finder. This is needed to enable subscriber usage of the SIP core services. This functionality is independent of the access network used to access the SIP core; and
- authentication functionality required by the SIP core to authenticate the MCPTT UE.

7.4.3.2.2 SIP database logical functions

The SIP database provides the following logical functions:

a) mobility management;
   - provides the UE mobility through the SIP core.

b) registrar assignment support;
   - provides to the registrar finder the required capabilities for MCPTT Services based on MCPTT service provider requirements on a per-user basis, (e.g. whether a particular registrar within the PLMN operator"s network (e.g. a registrar reserved for MCPTT use or a registrar in a secure location) or a registrar within the MCPTT service provider network is assigned.

c) call and/or session establishment support;
   - provides the call and/or session establishment procedures in the SIP core. For terminating traffic, it provides information on which registrar currently hosts the user.

d) user security information generation;
   - provides generation of user authentication, integrity and ciphering data for the SIP core.

e) signalling plane security support;
   - provides authentication procedures to access MCPTT services by storing the generated data for authentication, integrity and ciphering at the signalling plane and by providing these data to the appropriate registrar.

f) user identification handling;
   - provides the appropriate relations among all the identifiers uniquely determining the signalling plane identities in the SIP core e.g. IMS public identities.

g) access authorisation; and
   - provides authorisation of the user for mobile access when requested by the registrar e.g. by checking that the user is allowed to roam to that visited network.

h) service authorisation support.
   - provides basic authorisation for terminating call/session establishment and service invocation. The SIP database may update the registrar with filter criteria to trigger the MCPTT Server.

7.4.3.3 HTTP entities

7.4.3.3.1 HTTP client

This functional entity acts as the client for all hypertext transactions.

7.4.3.3.2 HTTP proxy

This functional entity acts as the proxy for all hypertext transactions between the HTTP client and HTTP server. The HTTP proxy terminates the TLS session on HTTP-1 with the HTTP client of the MCPTT UE in order to allow the HTTP client to establish a single TLS session for hypertext transactions with multiple HTTP servers.

Editor's note: Whether Identity management shares the same security domain as the rest of the common services core and whether there is an additional HTTP proxy for identity management is FFS.

The HTTP proxy shall be in the same trust domain as the HTTP clients and HTTP servers that are located within a MCPTT service provider"s network.

NOTE: The number of instances of the HTTP proxy is deployment specific.

7.4.3.3.3 HTTP server

This functional entity acts as the HTTP server for all hypertext transactions.

7.5 Reference points

7.5.1 General reference point principle

The protocols on any reference point that is exposed for MCPTT interoperability with other SIP core or other IMS entities in other systems shall be compatible with the protocols defined for the corresponding reference point defined in 3GPP TS 23.002 [3].

7.5.2 Application plane

7.5.2.1 General

The reference points for the application plane are described in the following subclauses.

7.5.2.2 Reference point MCPTT-1 (between the MCPTT client and the MCPTT server)

The MCPTT-1 reference point, which exists between the MCPTT client and the MCPTT server, is used for MCPTT application signalling for establishing a session in support of MCPTT. The MCPTT-1 reference point shall use the SIP-1 and SIP-2 reference points for transport and routing of SIP signalling. The MCPTT-1 reference point may use the HTTP-1 and HTTP-2 reference points.

Reference point MCPTT-1 may also provide the MCPTT server with location information with respect to multicast service availability for the MCPTT client. The TMGI is communicated between the MCPTT server and the MCPTT client using the MCPTT-1 reference point.

Information that is reported to the MCPTT server from the MCPTT client shall be configurable at the application layer. This interface may include the area where a UE is currently located, described as ECGI of the serving and neighbouring cell(s), SAIs, MBSFN Area ID. This information comes from the broadcast by the local cell, e.g. from SIB1 and SIB15 (see 3GPP TS 36.331 [14]) as decoded by the UE.

NOTE: This reference point includes the GC1 reference point as described in 3GPP TS 23.468 [10]. It is assumed that the MCPTT server is performing the function of GCS AS. While 3GPP TS 23.468 [10] does not specify GC1 it does include high level descriptions of certain interactions on GC1, including those relating to the availability of multicast delivery for the application client. The MCPTT-1 reference point fulfils the requirements of the GC1 reference point for MCPTT.

Messages supported on this interface may also include the MCPTT server providing the MCPTT client with information describing the mapping of transport resources to specific group calls.

7.5.2.3 Reference point MCPTT-2 (between the MCPTT server and the MCPTT user database)

The MCPTT-2 reference point, which exists between the MCPTT server and the MCPTT user database, is used by the MCPTT server to obtain information about a specific user. The MCPTT-2 reference point utilises the Sh reference point as defined in 3GPP TS 23.002 [3].

7.5.2.4 Reference point MCPTT-3 (between the MCPTT server and the MCPTT server)

The MCPTT-3 reference point, which exists between the MCPTT server and the MCPTT server for MCPTT application signalling for establishing MCPTT sessions, shall use the SIP-2 reference point for transport and routing of signalling. If each MCPTT server is served by a different SIP core then the MCPTT-3 reference point shall also use the SIP-3 reference point for transport and routing of signalling. Floor control signalling and media are also transferred using the MCPTT-3 reference point.

7.5.2.5 Reference point MCPTT-4 (unicast between the floor control server and the floor participant)

The MCPTT-4 reference point, which exists between the floor control server in the MCPTT server and the floor participant in the MCPTT client, provides floor control signalling between the floor control server in the MCPTT server and the floor participant over a unicast bearer. The MCPTT-4 reference point uses the SGi reference point defined in 3GPP TS 23.002 [3].

7.5.2.6 Reference point MCPTT-5 (between the media distribution function and the EPS)

The MCPTT-5 reference point, which exists between the media distribution function and the EPS, is used, subject to the conditions below, by the media distribution function of the MCPTT server to obtain unicast bearers with appropriate QoS from the EPS. It utilises the Rx interface of the EPS according to 3GPP TS 23.203 [4].

MCPTT-5 is not used when the MCPTT service provider and the PLMN operator do not have an operational agreement for QoS control to be provided directly from the MCPTT service provider domain.

MCPTT-5 may be used when the MCPTT service provider and the PLMN operator have an operational agreement where QoS control is provided directly from the MCPTT service provider domain.

NOTE: Any coordination between the P-CSCF use of Rx and the MCPTT server use of Rx (via MCPTT-5) from the MCPTT service provider domain is not specified in this release of this specification.

7.5.2.7 Reference point MCPTT-6 (between the MCPTT server and the EPS)

The MCPTT-6 reference point, which exists between the MCPTT server and the EPS, is used to request the allocation and activation of multicast transport resources for MCPTT application usage. The MCPTT-6 reference point uses the MB2-C interface as defined in 3GPP TS 29.468 [12].

7.5.2.8 Reference point MCPTT-7 (unicast between the media distribution function and the media mixer)

The MCPTT-7 reference point, which exists between the media distribution function and the media mixer, is used to exchange unicast media between the media distribution function of the MCPTT server and the media mixer of the MCPTT client. The MCPTT-7 reference point uses the SGi reference point defined in 3GPP TS 23.002 [3].

7.5.2.9 Reference point MCPTT-8 (multicast between the media distribution function and the media mixer)

The MCPTT-8 reference point, which exists between the media distribution function and the media mixer, is used by the media distribution function of the MCPTT server to send multicast media to the media mixer of the MCPTT client. The MCPTT-8 reference point uses the MB2-U interface defined in 3GPP TS 23.468 [10].

7.5.2.10 Reference point MCPTT-9 (multicast between the floor control server and the floor participant)

The MCPTT-9 reference point, which exists between the floor control server and the floor participant, provides floor control signalling between the floor control server and the floor participant over a multicast bearer. The MCPTT-9 reference point uses the MB2-U interface defined in 3GPP TS 23.468 [10].

7.5.2.11 Reference point CSC-1 (between the identity management client and the identity management server)

The CSC-1 reference point, which exists between the identity management client and the identity management server, provides for the authentication of the common services core to the MCPTT client and subsequent authentication of the user to the common services core on behalf of applications within the application plane.

CSC-1 is specified in 3GPP TS 33.179 [13].

7.5.2.12 Reference point CSC-2 (between the group management client and the group management server for configuration while UE is on-network)

The CSC-2 reference point, which exists between the group management client and the group management server, is used for MCPTT application signalling for MCPTT data management of the MCPTT service.

The CSC-2 reference point supports:

- Configuration of group related data at the group management client by the group management server; and
- Configuration of group related data at the group management server by the group management client.

The CSC-2 reference point shall use the HTTP-1 and HTTP-2 reference points for transport and routing of non-subscription/notification related signalling. The CSC-2 reference point shall use SIP-1 and SIP-2 reference points for transport and routing of subscription/notification related signalling.

7.5.2.13 Reference point CSC-3 (between the MCPTT server and the group management server)

The CSC-3 reference point, which exists between the MCPTT server and the group management server, provides for the MCPTT server to obtain group information. The CSC-3 reference point shall use HTTP-1 and HTTP-2 reference points for transport and routing of non-subscription/notification related signalling. The CSC-3 reference point shall use SIP-2 reference point for transport and routing of subscription/notification related signalling.

7.5.2.14 Reference point CSC-4 (between the configuration management client and the configuration management server for configuration while UE is on-network)

The CSC-4 reference point, which exists between the configuration management client and the configuration management server, provides the configuration information required for MCPTT services while the MCPTT client is on-network.

The CSC-4 reference point supports:

- configuration of the MCPTT UE by the MCPTT service; and
- configuration of the MCPTT application MCPTT service related information that is not part of group management (e.g. policy information) by the MCPTT UE.

The CSC-4 reference point shall use the HTTP-1 and HTTP-2 reference points for transport and routing of non-subscription/notification related signalling. The CSC-4 reference point shall use SIP-1 and SIP-2 reference points for transport and routing of subscription/notification related signalling.

7.5.2.15 Reference point CSC-5 (between the MCPTT server and the configuration management server)

The CSC-5 reference point, which exists between the MCPTT server and the configuration management server, provides for the MCPTT server to obtain non-group MCPTT service related information (e.g. policy information). The CSC-5 reference point shall use HTTP-1 reference point and HTTP-2 reference point for transport and routing of non-subscription/notification related signalling. The CSC-5 reference point shall use SIP-2 reference point for transport and routing of subscription/notification related signalling.

7.5.2.16 Reference point CSC-6 (between the identity management server and the MCPTT server)

The CSC-6 reference point, which exists between the identity management server and the MCPTT server, provides a means for the MCPTT server and the identity management server to share user identity information.

CSC-6 is specified in 3GPP TS 33.179 [13].

7.5.2.17 Reference point CSC-7 (between the group management server and the group management server)

The CSC-7 reference point, which exists between group management servers, allows group management servers to handle group management related signalling in multiple MCPTT systems environment. The CSC-7 reference point shall use the HTTP-1, HTTP-2 and HTTP-3 reference points for transport and routing of non-subscription/notification related signalling. The CSC-7 reference point shall use SIP-2 and SIP-3 reference points for transport and routing of subscription/notification related signalling.

7.5.2.18 Reference point CSC-8 (between the key management server and the key management client)

The CSC-8 reference point, which exists between the key management server and the key management client, provides a means for the key management server to provide security related information (e.g. encryption keys) to the key management client.

The CSC-8 reference point shall use the HTTP-1 and HTTP-2 reference points for transport and routing of security related information to the key management client.

CSC-8 is specified in 3GPP TS 33.179 [13].

7.5.2.19 Reference point CSC-9 (between the key management server and the MCPTT server)

The CSC-9 reference point, which exists between the key management server and the MCPTT server, provides a means for the key management server to provide security related information (e.g. encryption keys) to the MCPTT server.

The CSC-9 reference point shall use the HTTP-1 and HTTP-2 reference points for transport and routing of security related information to the group management server and MCPTT server.

CSC-9 is specified in 3GPP TS 33.179 [13].

7.5.2.20 Reference point CSC-10 (between the key management server and the group management server)

The CSC-10 reference point, which exists between the key management server and the group management server, provides a means for the key management server to provide security related information (e.g. encryption keys) to the group management server.

The CSC-10 reference point shall use the HTTP-1 and HTTP-2 reference points and may use the HTTP-3 reference point for transport and routing of security related information to the group management server and MCPTT server.

CSC-10 is specified in 3GPP TS 33.179 [13].

7.5.2.21 Reference point CSC-11 (between the configuration management client and the configuration management server for configuration while UE is off-network)

The CSC-11 reference point, which exists between the configuration management client and the configuration management server, provides the configuration information required for MCPTT services while the MCPTT client is off-network.

The CSC-11 reference point is the same as CSC-4 reference point except that CSC-11 does not support subscription/notification and therefore does not require the use of SIP-1 and SIP-2 reference points.

7.5.2.22 Reference point CSC-12 (between the group management client and the group management server for configuration while UE is off-network)

The CSC-12 reference point, which exists between the group management client and the group management server, is used for MCPTT application signalling for MCPTT data management of the MCPTT service.

The CSC-12 reference point is the same as CSC-2 reference point except that CSC-12 does not support subscription/notification and therefore does not require the use of SIP-1 and SIP-2 reference points.

7.5.2.23 Reference point CSC-13 (between the configuration management server and the MCPTT user database)

The CSC-13 reference point, which exists between the MCPTT user database and the configuration management server, is used for:

- the configuration management server to store the user profile data in the MCPTT user database; and
- the configuration management server to obtain the user profile from the MCPTT user database for further configuration in the MCPTT UE.

7.5.2.24 Reference point IWF-1 (between the MCPTT server and the interworking function to legacy systems)

The IWF-1 reference point, which exists between the MCPTT server and the interworking function to legacy systems, is not specified in the present document.

NOTE: A subset of the functionality provided by the existing MCPTT reference points could be used to interconnect with legacy systems.

7.5.3 Signalling control plane

7.5.3.1 General

The reference points for the SIP and HTTP signalling are described in the following subclauses.

7.5.3.2 Reference point SIP-1(between the signalling user agent and the SIP core)

The SIP-1 reference point, which exists between the signalling user agent and the SIP core for establishing a session in support of MCPTT, shall use the Gm reference point as defined in 3GPP TS 23.002 [3] (with necessary enhancements to support MCPTT requirements and profiled to meet the minimum requirements for support of MCPTT). The SIP-1 reference point fulfils the requirements of the GC1 reference point specified in3GPP TS 23.468 [10]. The SIP-1 reference point is used for:

- SIP registration;
- authentication and security to the service layer;
- event subscription and notification;

- communication of the TMGI for multicast operation;
- overload control; and
- session management and media negotiation.

7.5.3.3 Reference point SIP-2 (between the SIP core and the SIP AS)

The SIP-2 reference point, which exists between the SIP core and the SIP AS for establishing a session in support of MCPTT, shall use the ISC and Ma reference points as defined in 3GPP TS 23.002 [3]. The SIP-2 reference point is used for:

- notification to the MCPTT server of SIP registration by the MCPTT UE;
- authentication and security to the service layer;
- event subscription and notification;
- communication of the TMGI for multicast operation; and
- session management and media negotiation.

7.5.3.4 Reference point SIP-3 (between the SIP core and SIP core)

The SIP-3 reference point, which exists between one SIP core and another SIP core for establishing a session in support of MCPTT, shall use the Mm and ICi reference points as defined in 3GPP TS 23.002 [3]. The SIP-3 reference point is used for:

- event subscription and notification; and
- session management and media negotiation.

7.5.3.5 Reference point HTTP-1 (between the HTTP client and the HTTP proxy)

The HTTP-1 reference point exists between the HTTP client and the HTTP proxy. Between the MCPTT UE and the HTTP proxy, the HTTP-1 reference point shall use the Ut reference point as defined in 3GPP TS 23.002 [3] (with necessary enhancements to support MCPTT requirements). The HTTP-1 reference point is based on HTTP (which may be secured using e.g. SSL, TLS).

7.5.3.6 Reference point HTTP-2 (between the HTTP proxy and the HTTP server)

The HTTP-2 reference point, which exists between the HTTP proxy and the HTTP server, is based on HTTP (which may be secured using e.g. SSL, TLS).

7.5.3.7 Reference point HTTP-3 (between the HTTP proxy and HTTP proxy)

The HTTP-3 reference point, which exists between the HTTP proxy and another HTTP proxy in a different network, is based on HTTP (which may be secured using e.g. SSL, TLS).

7.5.3.8 Reference point AAA-1 (between the SIP database and the SIP core)

The AAA-1 reference point, which exists between the SIP database and the SIP core, is used by the SIP core to retrieve signalling plane data from the SIP database. The AAA-1 reference point utilises the Cx reference point as defined in 3GPP TS 23.002 [3].

In some deployment scenarios the registrar and SIP database are located in the MCPTT service provider's network while the registrar finder is in the PLMN operator's network and the AAA-1 reference point is an inter-network interface.

8 Identities

8.1 Application plane

8.1.1 Mission Critical user identity (MC ID)

The mission critical user identity is also known as the MC ID. The MC ID is the identity that an MCPTT user presents to the identity management server during a user authentication transaction. In general, since identity management is a common service it uses an identity which is linked to a set of credentials (e.g. biometrics, secureID, username/password) that may not necessarily be tied to a single mission critical service. The MC ID and the MCPTT ID may be the same. The MC ID uniquely identifies the MCPTT user to the identity management server. The MC ID is used by the identity management server to provide the identity management client a means for mission critical service authentication.

NOTE: The specific security and authentication mechanisms required in order to use the MC user identity is specified in 3GPP TS 33.179 [13].

8.1.2 MCPTT user identity (MCPTT ID)

The MCPTT user identity is also known as the MCPTT ID. The MCPTT ID is a globally unique identifier within the MCPTT service that represents the MCPTT user. The MCPTT ID identifies an MCPTT user. The MCPTT ID may also identify an MCPTT profile for the user at the MCPTT application layer.

There are attributes associated with the MCPTT ID configured in the MCPTT service that relate to the human user of the MCPTT service. Typically this information identifies the MCPTT user, by name or role, and may also identify a user's organization or agency. Such attributes associated with an MCPTT ID can be used by the MCPTT server to make authorization decisions about the MCPTT service granted to the user. For example, an attribute that identifies a user's role as an incident commander could automatically be used by the MCPTT service to grant the user additional administrative rights over the creation of groups, or access to privileged talk groups.

The MCPTT ID shall be a URI. The MCPTT ID uniquely identifies an MCPTT user in an MCPTT system. The MCPTT ID indicates the MCPTT system where the MCPTT ID is defined.

When required by the MCPTT service provider, the MCPTT ID is hidden from the signalling control plane.

A default or temporary MCPTT ID may be used where a user is not yet associated with a device. When a user would like to use MCPTT services but has not been authenticated by the identity management server, a default or temporary MCPTT ID and a corresponding MCPTT user profile may be used.

8.1.3 MCPTT group identity (MCPTT group ID)

8.1.3.1 General

The MCPTT group identity is also known as the MCPTT group ID. The MCPTT group ID is a globally unique identifier within the MCPTT service that represents a set of MCPTT users. The set of MCPTT users may belong to the same or different MCPTT systems. The MCPTT system for each user (within the group) is identified by each user's respective MCPTT ID.

The MCPTT group ID identifies an MCPTT group in an MCPTT system. It indicates both the MCPTT system where the MCPTT group is defined, and the MCPTT server within the MCPTT system where the group is defined.

The MCPTT group ID is used as follows:

a) For identifying a set of identities of its group members; and

b) By the MCPTT client to address the MCPTT group.

The MCPTT group ID shall be a URI.

When required by the MCPTT service provider, the MCPTT group ID is hidden from the signalling control plane.

8.1.3.2 MCPTT group ID management (off-network operation)

In off-network operation, an MCPTT group ID is used for identifying the MCPTT group while off-network. The MCPTT group ID should be resolved to the ProSe Group IP multicast address and ProSe Layer-2 Group ID for the group communication. The MCPTT UE is able to make communication with other member UEs whose users are of the same MCPTT group ID over ProSe direct communications based on ProSe Layer-2 Group ID and ProSe Group IP multicast address, as described in 3GPP TS 3GPP 23.303 [8].

Figure 8.1.3.2-1 illustrates how the MCPTT group ID, ProSe Group IP multicast address and the ProSe Layer-2 Group ID are mapped to each other. ProSe Group IP multicast address and ProSe Layer-2 Group ID are pre-configured in accordance with the MCPTT group ID. Thus, they are pre-defined and associated. This mapping information should be provisioned through UICC in the UE or through ProSe function as specified in 3GPP TS 23.303 [8], or be delivered from an application server. Mapping information is provisioned from group management server in case of online configuration, and provisioned from configuration management server in case of offline configuration.

NOTE: To define the retrieval mechanism of the off-network information (ProSe Group IP multicast address and ProSe Layer-2 Group ID) from ProSe function to group management server is out of scope of the present document.

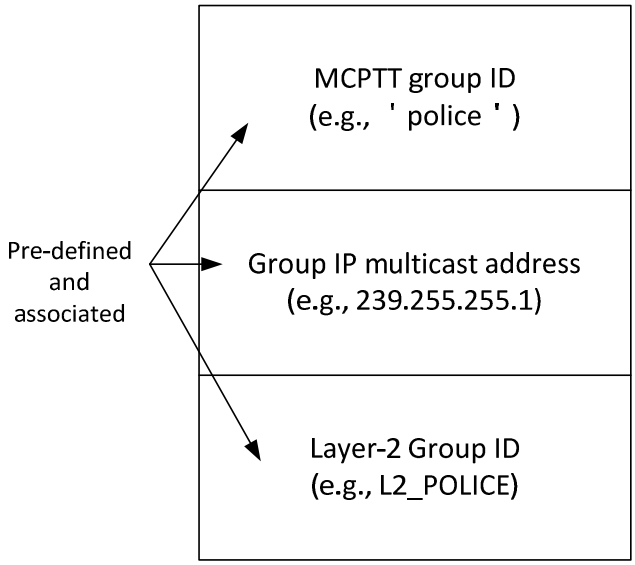

Figure 8.1.3.2-1: MCPTT group ID management in off-network operation

8.2 SIP signalling control plane

The SIP signalling control plane depends upon the use of both a private user identity and one or more public user identities.

When the signalling user agent sends registration requests to the registrar / application service selection, the private user identity is used to find corresponding credentials for authentication of the signalling user agent by the registrar / application service selection. This private user identity fulfils the same functions as the IMPI defined in 3GPP TS 23.228 [5].

All SIP signalling messages sent by a signalling user agent to an MCPTT server via a SIP core use a public user identity as the identifier to enable signalling messages to be routed through the SIP system. The public user identity fulfils the same functions as IMPU defined in 3GPP TS 23.228 [5].

The public user identities do not necessarily contain any MCPTT application-level attributes (e.g., MCPTT ID). Any association of the public user identities with such attributes occurs at the application layer only.

When the SIP core and the MCPTT service are part of the same trust domain, public user identities may be provided by the MCPTT service provider, or the PLMN operator. When the SIP core and the MCPTT service are part of the different trust domains, public user identities may be provided by the PLMN operator.

NOTE: The MCPTT service provider can have an agreement with the PLMN operator to manage a pool of public user identities.

The SIP core may generate public GRUUs and temporary GRUUs in order to uniquely identify MCPTT UEs when a user logging on from multiple devices or multiple users sharing the same device is supported per 3GPP TS 23.228 [5].

Public service identity is used as the identifier to route SIP signalling for the MCPTT system. The public service identity fulfils the same functions as PSI defined in 3GPP TS 23.228 [5].

8.3 Relationship between identities in different planes

8.3.1 Relationship between MCPTT ID and public user identity

The following relationships exist between the MCPTT ID(s) and the public user identity(ies):

- An MCPTT ID may be mapped to one or more public user identities (e.g. multiple UEs, shared UE);
- A public user identity may be mapped to one or more MCPTT IDs (e.g. UE-to-network relay); and
- An MCPTT ID may be mapped to one or more public GRUUs (e.g. a user logging on from multiple UEs, multiple users sharing the same UE).

The MCPTT server manages the mapping between MCPTT IDs and public user identities.

The MCPTT server manages the mapping between MCPTT IDs and public GRUUs.

Temporary GRUUs are mapped to public GRUUs by the SIP core.

The public user identity does not necessarily identify the MCPTT user at the SIP signalling control plane. When the MCPTT service provider and the home PLMN operator are part of the same trust domain, the public user identity in the SIP signalling control plane may also identify the MCPTT user at the application plane.

8.3.2 Relationship between MCPTT group ID and public service identity

Each MCPTT group ID shall be mapped to a public service identity for the MCPTT server where the group is defined. The MCPTT server manages the mapping between MCPTT group IDs and public service identities.

When the MCPTT service provider and the home PLMN operator are part of the same trust domain, the public service identity in the SIP signalling control plane may also identify the MCPTT group ID at the application plane.

9 Application of functional model to deployments

9.1 General

This clause describes the application of the functional model, described in clause 7, to on-network and off-network deployments. It also describes deployment scenarios that highlight some of the possible variations in the way that the functional model can be applied in different situations.

9.2 Architecture model and deployment scenarios for on-network operations

9.2.1 On-network architectural model

9.2.1.1 On-network architectural model diagram

Figure 9.2.1.1-1 below is the on-network architectural model for the MCPTT system solution, where the MCPTT system provides MCPTT service via a single PLMN.

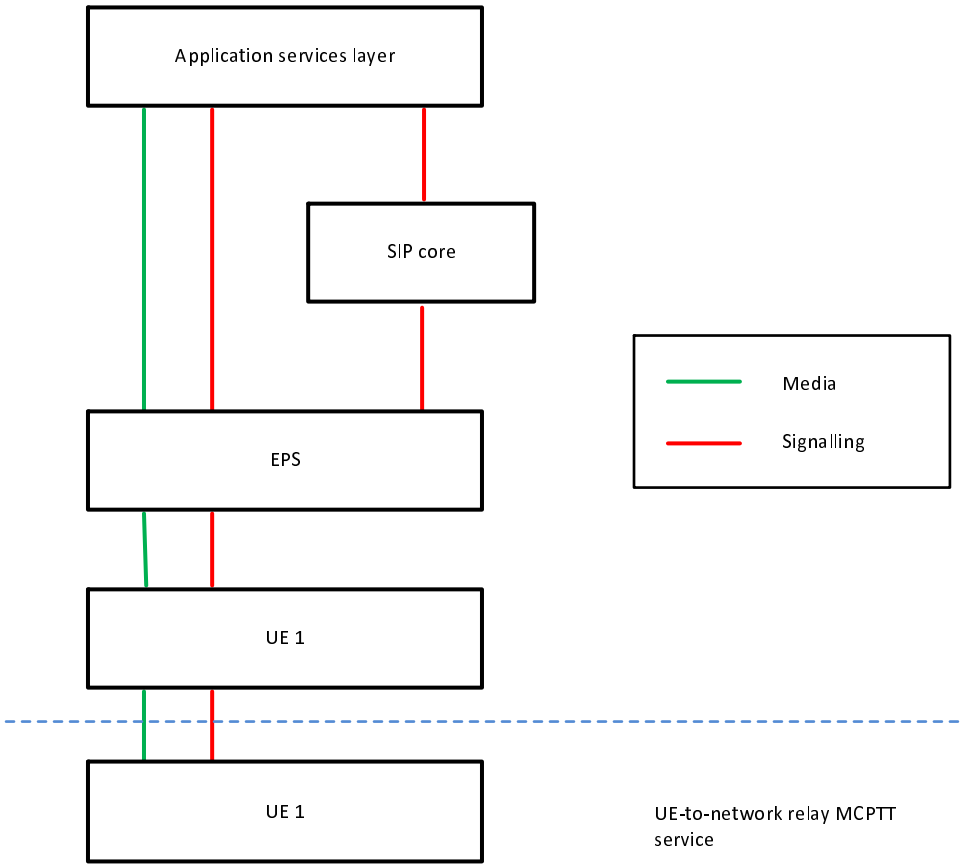

Figure 9.2.1.1-1: On-network architectural model

9.2.1.2 Application services layer

9.2.1.2.1 Overview

The application services layer includes MCPTT application and any required supporting functions grouped into common services core.

9.2.1.2.2 Common services core

Common services core is composed of the following functional entities:

- for common services, a configuration management server as described in subclause 7.4.2.2.2, a group management server as described in subclause 7.4.2.2.4 and an identity management server as described in subclause 7.4.2.2.6; and

- for signalling control, an HTTP proxy as described in subclause 7.4.3.3.2 and an HTTP server as described in subclause 7.4.3.3.3.

9.2.1.2.3 MCPTT application service

MCPTT application service is composed of the following functional entities:

- an MCPTT server as described in subclause 7.4.2.3.2; and
- for media, a floor control server as described in subclause 7.4.2.3.4 and a media distribution function as described in subclause 7.4.2.3.5.

9.2.1.3 SIP core

The SIP core provides rendezvous (contact address binding and URI resolution) and service control (application service selection) functions. It is composed of the following functional entities:

- for signalling control, a local inbound / outbound proxy as described in subclause 7.4.3.1.3.2, a registrar finder as described in subclause 7.4.3.1.3.3 and a registrar / application service selection entity as described in subclause 7.4.3.1.3.4.

9.2.1.4 EPS

The EPS provides point-to-point and point-to-multipoint bearer services with QoS.

9.2.1.5 UE 1

UE 1 is:

- a device supporting bearer services and application(s) related to MCPTT;
- a device that acts as ProSe UE-to-network relay; or
- both of the above.

When acting as a device supporting bearer services and application(s) related to MCPTT, UE 1 is composed of the same functional entities as for UE 2, as described in subclause 9.2.1.6.

9.2.1.6 UE 2

UE 2 is a device using ProSe UE-to-network relay, and supporting application(s) related to MCPTT. It is composed of the following functional entities:

- for common services, a group management client as described in subclause 7.4.2.2.3, a configuration management client as described in subclause 7.4.2.2.1 and an identity management client as described in subclause 7.4.2.2.5;
- for MCPTT application services, an MCPTT client as described in subclause 7.4.2.3.1;
- for signalling control, a signalling user agent as described in subclause 7.4.3.1.1 and an HTTP client as described in subclause 7.4.3.3.1; and
- for media, a floor participant as described in subclause 7.4.2.3.3.

9.2.2 Deployment scenarios

9.2.2.1 Administration of MCPTT application service, SIP core and EPS

9.2.2.1.1 General

This subclause describes five different deployment scenarios in which different administration of MCPTT application service, SIP core and EPS are described, together with the sensitivities of identities and other forms of signalling in those scenarios.

In each of these scenarios, the owner of the devices at each plane may be different from the organisation that administers these devices. For example, the MCPTT service provider may own some RAN components within the EPS even when the EPS is administered by the PLMN operator, and the MCPTT UE may be owned by an organisation that is independent from PLMN and MCPTT service providers.

9.2.2.1.2 Common administration of all planes

In this scenario, all planes (application services layer, SIP core and EPS) are administered by the same party. This is illustrated in figure 9.2.2.1.2-1 below.

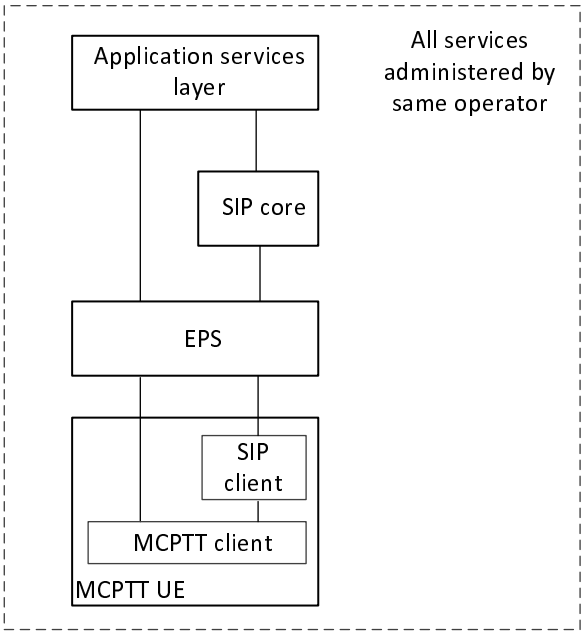

Figure 9.2.2.1.2-1: Common administration of all services by one operator

Although the identities in each plane are separate according to clause 8, there is no particular sensitivity of identities and other information at the application plane, and these may be exposed to the SIP core and the EPS.

All authorisation and authentication mechanisms at each plane, i.e. the application services layer, SIP core and EPS, shall be separate, but there may be no need for any restrictions in how these are stored and managed; for example the same entity could provide services to each of the application services layer, SIP core and EPS.

9.2.2.1.3 MCPTT service provider separate from SIP core and EPS

In this scenario, as illustrated in figure 9.2.2.1.3-1, the MCPTT service provider is separate and independent from the PLMN operator, and the MCPTT service is administered independently of the EPS and SIP core. The PLMN operator administers the EPS and the SIP core.

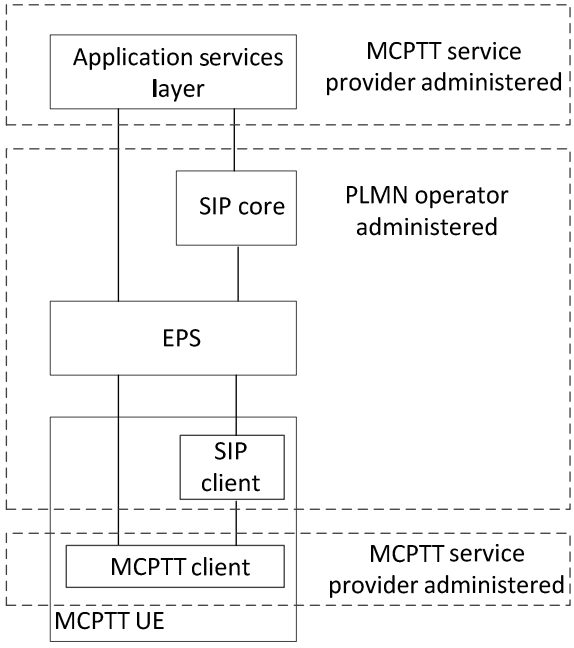

Figure 9.2.2.1.3-1: MCPTT service provider administers MCPTT service separately from SIP core and EPS

The MCPTT service provider may require that all application services layer identities and other sensitive information are hidden both from the SIP core and the EPS.

When required by the MCPTT service provider, all authentication and authorisation mechanisms, including security roots, at the application services layer are hidden from and not available to the PLMN operator.

9.2.2.1.4 MCPTT service provider administers SIP core, separate from EPS

In this scenario, as illustrated in figure 9.2.2.1.4-1, the MCPTT service provider administers the SIP core, and the MCPTT application services and SIP core are independent of the PLMN operator.

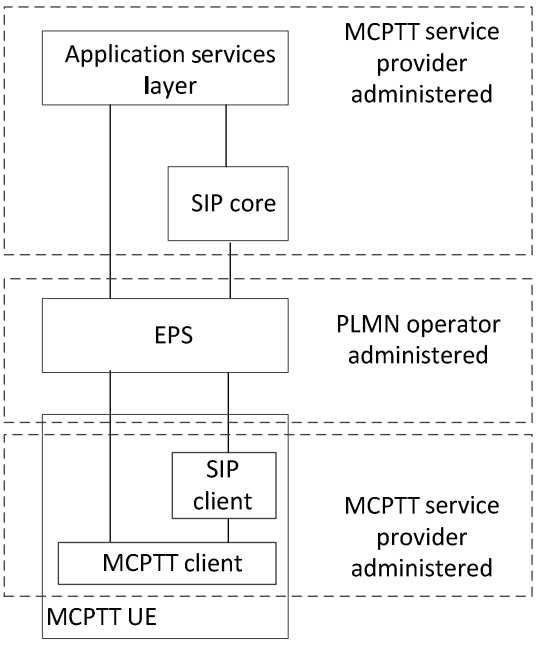

Figure 9.2.2.1.4-1: MCPTT provision of SIP core, separate domain from EPS

The MCPTT service provider may require that all identities and other sensitive information at the application services layer are hidden from the EPS. The MCPTT service provider need not hide the identities and signalling at the

application services layer from the SIP core. However the MCPTT service provider may require that identities and other sensitive information between SIP core and SIP client in the MCPTT UE are also hidden from the EPS.

All authentication and authorisation mechanisms, including security roots, at both application services layer and at SIP signalling plane may need to be hidden from, and not available to, the PLMN operator.

9.2.2.1.5 SIP core partially administered by both PLMN operator and MCPTT service provider

In this scenario, as illustrated in figure 9.2.2.1.5-1, the SIP core is partially administered by both parties, for example when the SIP core registrar is administered by the MCPTT service provider, but the SIP core registrar finder and proxy is administered by the PLMN operator.

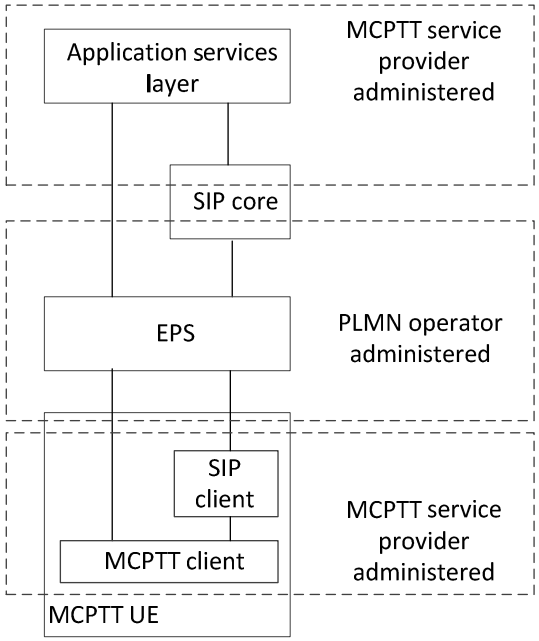

Figure 9.2.2.1.5-1: MCPTT service provider provision of SIP core, separate domain from EPS

The MCPTT service provider may require that all identities and signalling at the application services layer are hidden from the EPS, and may require identities and other sensitive information to be hidden from the PLMN operator administered part of the SIP core.

All authentication and authorisation mechanisms, including security roots, at the application services layer may need to be hidden from, and not available to, the PLMN operator.

9.2.2.1.6 PLMN operator administers SIP core with SIP identities administered by MCPTT service provider

In this scenario, the PLMN operator administers the SIP core. However, the identities used by the SIP core (IMPI and IMPU) for MCPTT UEs served by the MCPTT service provider are provided from the SIP database of the MCPTT service provider.

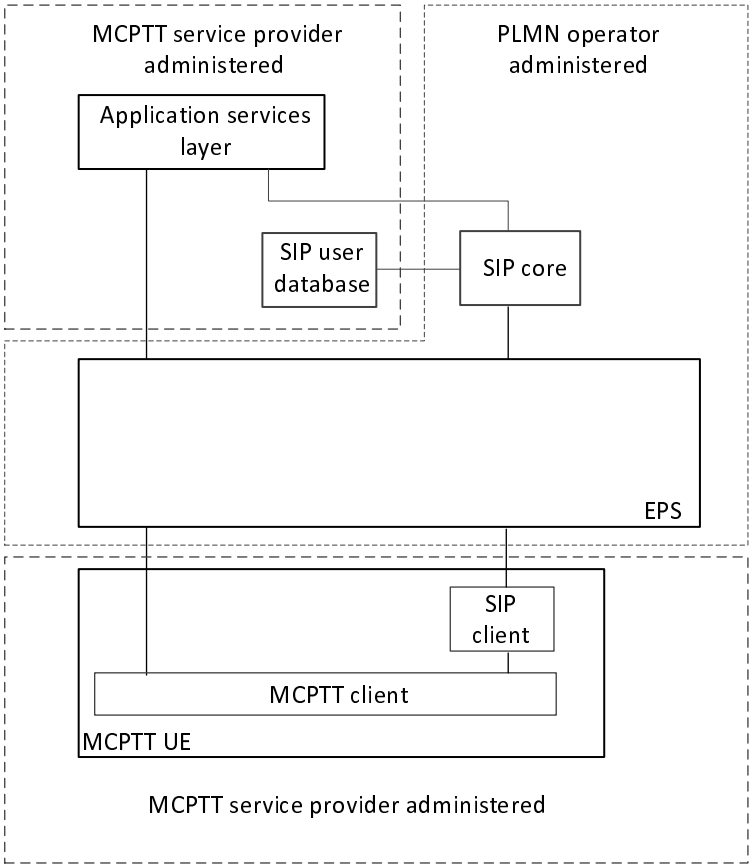

Figure 9.2.2.1.6-1: MCPTT service provider provides identities to PLMN operator SIP core

The MCPTT service provider may require that all identities and signalling at the application services layer are hidden from the SIP core and EPS.

When required by the MCPTT service provider, all authentication and authorisation mechanisms, including security roots, at the application services layer may need to be hidden from, and not available to, the PLMN operator.

The security roots (authentication keys) required for access to the signalling control plane are not available to the PLMN operator as these are held in the MCPTT service provider's SIP user database. However, derived parameters e.g. authentication vectors are provided to the SIP core to allow signalling control plane authentication to take place.

9.2.2.2 MCPTT user database, SIP database and HSS

Figures 9.2.2.2-1 to 9.2.2.2-4 show the possible deployment scenarios of the MCPTT user database and SIP user database, including collocation with the HSS.

NOTE: As an implementation option, the SIP database can be located within the SIP core, in which case the AAA-1/Cx interface is not exposed.

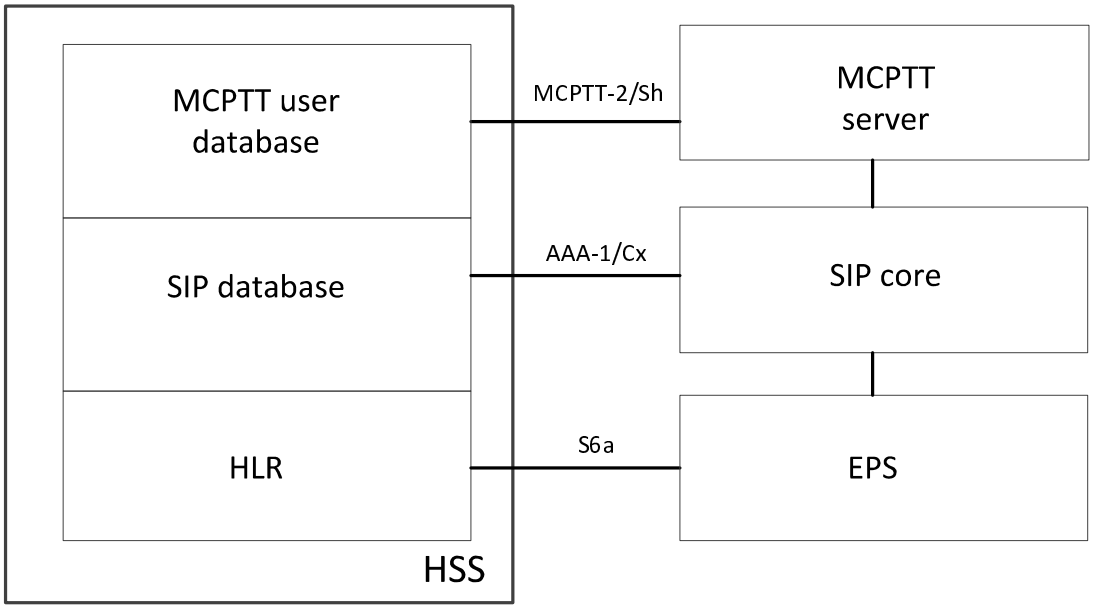

Figure 9.2.2.2-1: Collocation of MCPTT user database and SIP database with HSS

The HSS depicted in figure 9.2.2.2-1 can be deployed either in the PLMN operator's network or the MCPTT service provider's network.

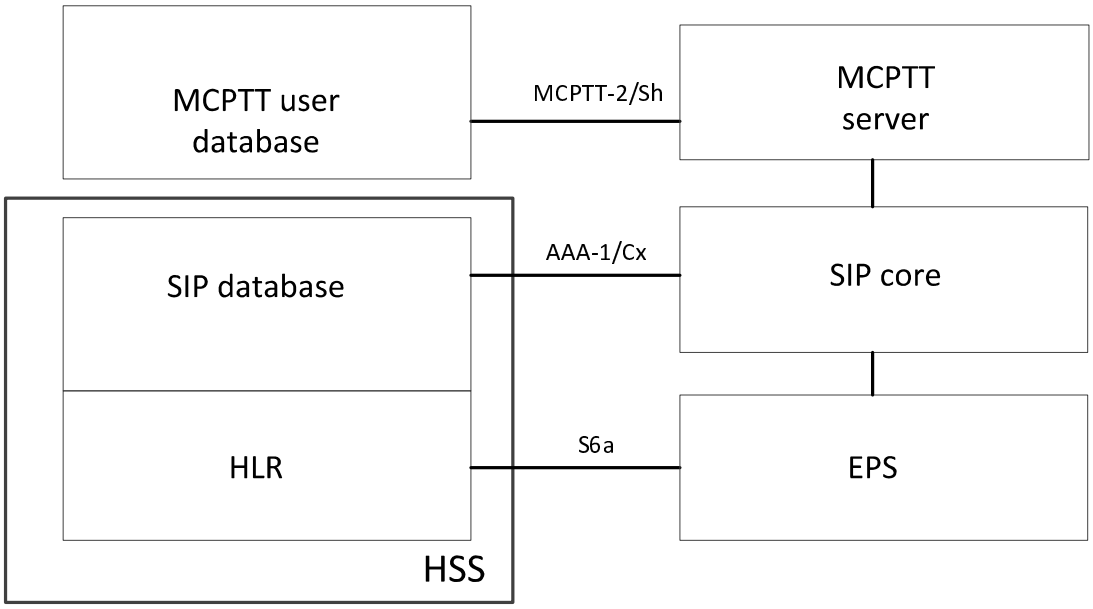

Figure 9.2.2.2-2: Shared PLMN operator and MCPTT service provider based deployment of MCPTT service - SIP database collocated with HSS with separate MCPTT user database

The MCPTT user database depicted in figure 9.2.2.2-2 can be deployed in the PLMN operator's network or the MCPTT service provider's network, and the HSS depicted in figure 9.2.2.2-2 can be deployed in the same or different network to the MCPTT user database i.e. PLMN operator's network or the MCPTT service provider's network.

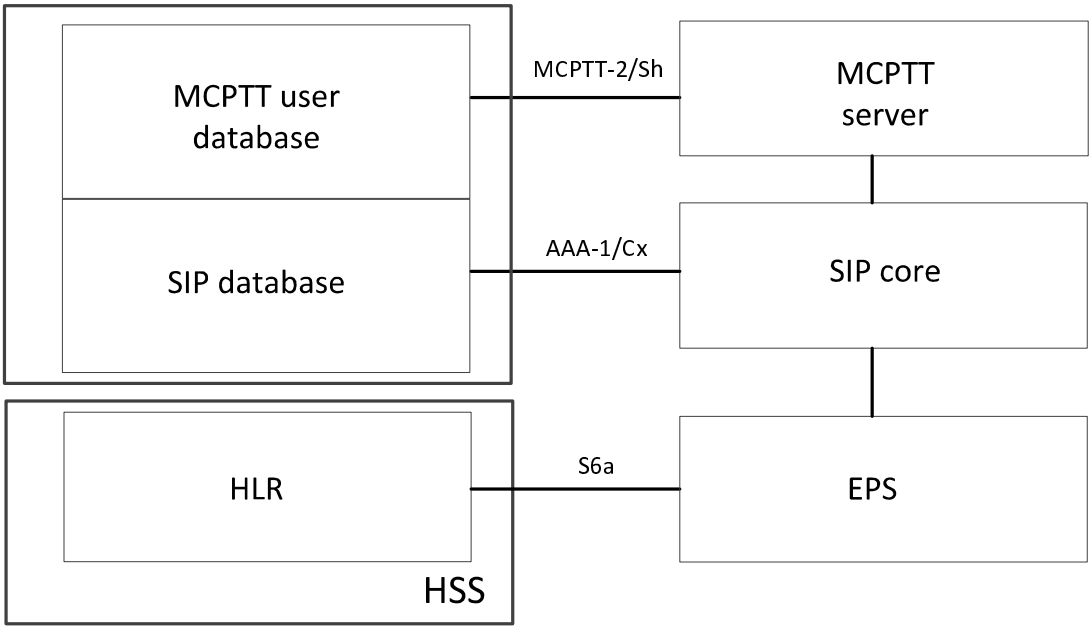

Figure 9.2.2.2-3: Shared PLMN operator and MCPTT service provider based deployment of MCPTT service - collocation of MCPTT user database and SIP database, with separate HSS

The MCPTT user database and SIP database depicted in figure 9.2.2.2-3 can be deployed in the PLMN operator's network or the MCPTT service provider's network, and the HSS depicted in figure 9.2.2.2-3 can be deployed in the same or different network to the MCPTT user database i.e. PLMN operator's network or the MCPTT service provider's network.

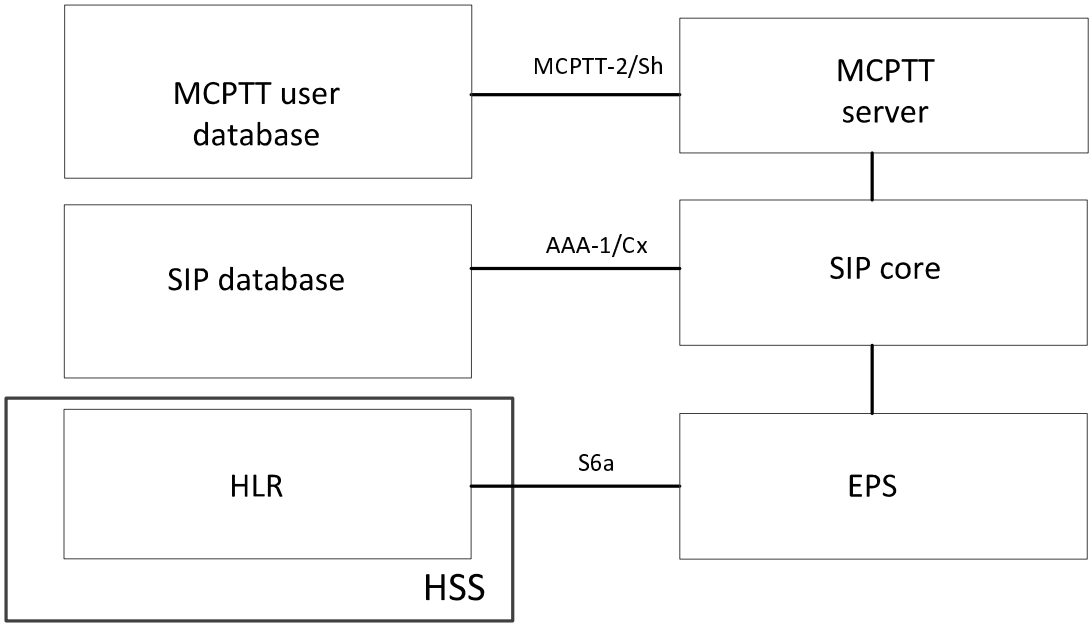

Figure 9.2.2.2-4: Shared PLMN operator and MCPTT service provider based deployment of MCPTT service - separate HSS, MCPTT user database and SIP database

Each of the MCPTT user database, SIP database and HSS depicted in figure 9.2.2.2-4 can be deployed in the same or different networks i.e. PLMN operator's network or the MCPTT service provider's network.

9.2.2.3 Control of bearers by SIP core and MCPTT server

9.2.2.3.1 General

This subclause describes two different scenarios in which bearers are controlled by access to Rx by either the SIP core or the MCPTT server.

These may provide suitable models for each of the scenarios listed in subclause 9.2.2.1. However, there is no direct correlation of any of the scenarios described in this subclause to each of the scenarios described in subclause 9.2.2.1.

9.2.2.3.2 Control of bearers by SIP core

In this scenario, bearer control is performed by the SIP core alone, as shown in figure 9.2.2.3.2-1 below.

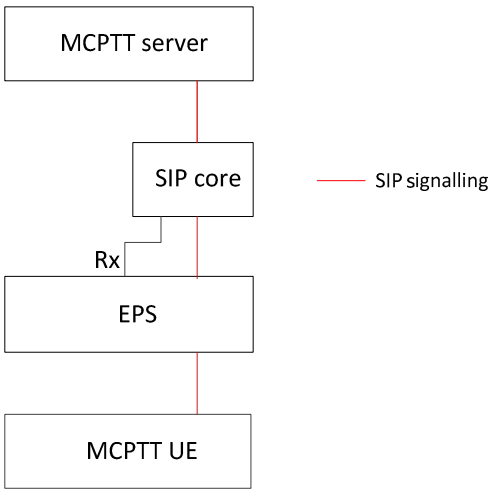

Figure 9.2.2.3.2-1: Bearer control by SIP core

9.2.2.3.3 Control of bearers by MCPTT server

In this scenario, bearer control is performed by the MCPTT server alone, as shown in figure 9.2.2.3.3-1 below.

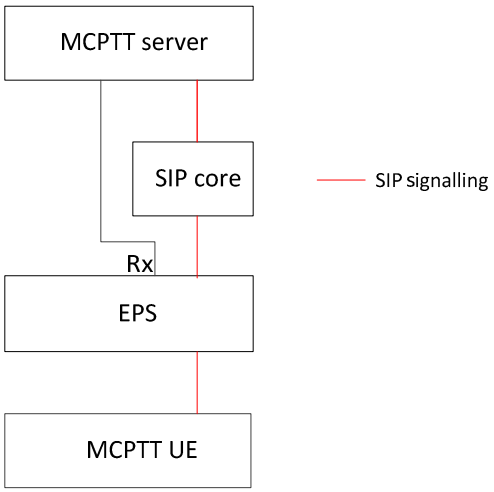

Figure 9.2.2.3.3-1: Bearer control by MCPTT server

9.3 Architecture model for off-network operations

9.3.1 Off-network architectural model diagram

Figure 9.3.1-1 shows the off-network architectural model for the MCPTT system solution for inter-UE communication, where no relay function is used.

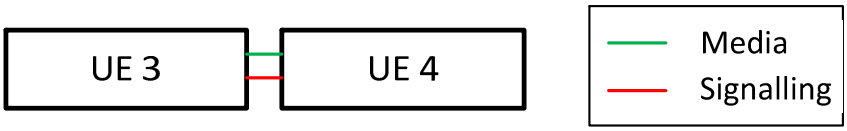

Figure 9.3.1-1: Off-network architectural model for inter-UE communication where no relay function is used

Figure 9.3.1-2 shows the off-network architectural model for the MCPTT system solution for configuration management and group management.

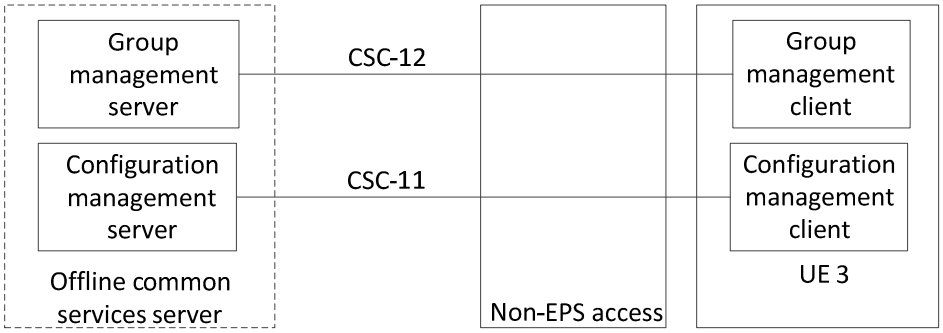

Figure 9.3.1-2: Off-network architectural model for configuration management and group management

NOTE 1: The offline common services server denoted in figure 9.3.1-2 could be provided by a portable device e.g. laptop.

NOTE 2: Non-EPS access can be any IP-CAN that is mutually supported by the offline common services server and the UE 3, and which provides necessary connectivity for the CSC-11 and CSC-12 reference points. It is out of scope of this specification what type of IP-CANs are supported, but could be e.g. USB, Bluetooth, WLAN.

NOTE 3: The offline common services server could be the same entity (or set of entities) as the common services core.

The entities within this model are described in the following subclauses and a full functional model is given in subclause 7.3.2.

9.3.2 UE 3

The UE 3 is a UE using ProSe and supporting application(s) related to off-network MCPTT service, and is composed of the following functional entities:

- for MCPTT application services, an MCPTT client as described in subclause 7.4.2.3.1;
- for signalling control, a signalling user agent as described in subclause 7.4.3.1.1;
- for configuration management, a configuration management client as described in subclause 7.4.2.2.1;
- for group management, a group management client as described in subclause 7.4.2.2.3; and

- for media, a floor participant as described in subclause 7.4.2.3.3 and, for distributed floor control, a floor control server as described in subclause 7.4.2.3.4.

9.3.3 UE 4

The UE 4 represents one or more UEs with the same functionality as UE 3.

9.3.4 Off-line common services server

The offline common services server supports configuration applications related to MCPTT service, and is composed of the following functional entities:

- for configuration management, a configuration management server as described in subclause 7.4.2.2.2; and
- for group management, a group management server as described in subclause 7.4.2.2.4.

9.4 Architecture model for roaming

Roaming is achieved using either:

- EPC-level roaming as defined in 3GPP TS 23.401 [9]; or
- IMS-level roaming as defined in 3GPP TS 23.228 [5].

10 Procedures and information flows

10.1 MCPTT configuration

10.1.1 General

Depicted in figure 10.1.1-1 is a MCPTT configuration time sequence of the data in Annex B, representing the general lifecycle of MCPTT UE using MCPTT service.

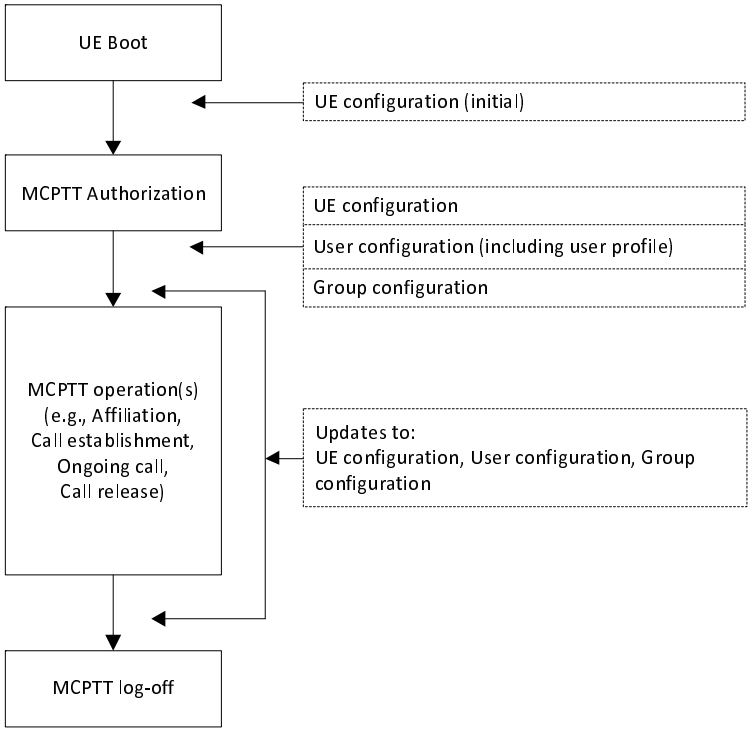

Figure 10.1.1-1 MCPTT UE configuration time sequence and associated configuration data

The online configuration to the MCPTT UE includes UE configuration, user configuration and group configuration. While the MCPTT UE is using the MCPTT service it may receive online configuration updates.

The MCPTT service is configured with the service configuration (not shown in the figure 10.1.1-1) which the MCPTT service enforces during the entire phase of MCPTT UE using the MCPTT service.

10.1.2 Information flows for MCPTT configuration

10.1.2.1 Store group configuration request

Table 10.1.2.1-1 describes the information flow store group configuration request from the group management client to the group management server.

Table 10.1.2.1-1: Store group configuration request

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the group
MCPTT group configuration data	M	MCPTT group configuration data

10.1.2.2 Store group configuration response

Table 10.1.2.2-1 describes the information flow store group configuration response from the group management server to the group management client.

Table 10.1.2.2-1: Store group configuration response

Information element	Status	Description
Result	M	Indicates the success or failure for the result

10.1.2.3 Store group configuration request

Table 10.1.2.3-1 describes the information flow store group configuration request from the group management server to the group management client.

Table 10.1.2.3-1: Store group configuration request

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the group
MCPTT group data	M	MCPTT group data.

10.1.2.4 Store group configuration response

Table 10.1.2.4-1 describes the information flow store group configuration response from the group management client to the group management server.

Table 10.1.2.4-1: Store group configuration response

Information element	Status	Description
Result	M	Indicates the success or failure for the result

10.1.2.5 Subscribe group configuration request

Table 10.1.2.5-1 describes the information flow subscribe group configuration request from the group management client to the group management server.

Table 10.1.2.5-1: Subscribe group configuration request

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the group

10.1.2.6 Subscribe group configuration response

Table 10.1.2.6-1 describes the information flow subscribe group configuration response from the group management server to the group management client.

Table 10.1.2.6-1: Subscribe group configuration response

Information element	Status	Description
Result	M	Indicates the success or failure for the result

10.1.2.7 Notify group configuration

Table 10.1.2.7-1 describes the information flow notify group configuration from the group management server to the group management client.

Table 10.1.2.7-1: Notify group configuration

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the group
MCPTT group configuration data	M	MCPTT group configuration data

10.1.3 MCPTT UE configuration data

10.1.3.1 General

The MCPTT UE configuration data has to be known by the MCPTT UE before it can use the MCPTT service.

10.1.3.2 Procedures

The procedure for MCPTT UE obtaining the MCPTT UE related configuration data is illustrated in figure 10.1.3.2-1.

Pre-conditions:

- The MCPTT UE has the secure access to the configuration management server.

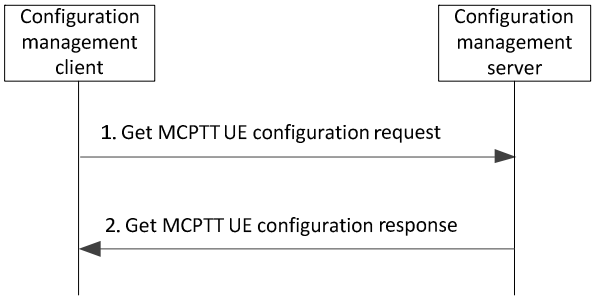

Figure 10.1..2-1: MCPTT UE obtains the configuration data

1. The configuration management client sends a get MCPTT UE configuration request to the configuration management server for obtaining MCPTT UE configuration data.
2. The configuration management server sends get MCPTT UE configuration response to the configuration management client. This message carries the MCPTT UE configuration data.

10.1.3.3 Structure of data

The MCPTT UE configuration data includes the following information elements:

- relay service (Y/N);
- the list of allowed relayed MCPTT groups (optional); and
- relay service code associated with each MCPTT group (as specified in 3GPP TS 23.303 [8]).

10.1.4 MCPTT user profile

10.1.4.1 General

An MCPTT user is associated with at least one MCPTT user profile and can be associated with several. The MCPTT user profile is stored in MCPTT user database. MCPTT user profile information is downloaded to the MCPTT UE. For the same MCPTT user there can be different MCPTT user profiles active on different MCPTT UEs or on the same MCPTT UE at different times. Only one MCPTT user profile per MCPTT client is active at a time.

Different parts of the MCPTT user profile are provisioned by the Mission Critical Organization, by the MCPTT service provider and by the MCPTT user, respectively. The MCPTT user profile provisioning can be initiated by MCPTT client (e.g. upon MCPTT user"s initial log on or on reconnect to MCPTT service), or initiated by MCPTT server (e.g. the dynamic attributes applied to MCPTT service due to role change or organization change).

Information contained in the MCPTT user profile is listed in annex B.

10.1.4.2 MCPTT user obtains the user profile (UE initiated)

The procedure for MCPTT user obtaining the user profile that is initiated by MCPTT UE is illustrated in figure 10.1.4.2-1.

Pre-conditions:

- The MCPTT user has performed user authentication in identity management server.
- The MCPTT UE has the secure access to the configuration management server.

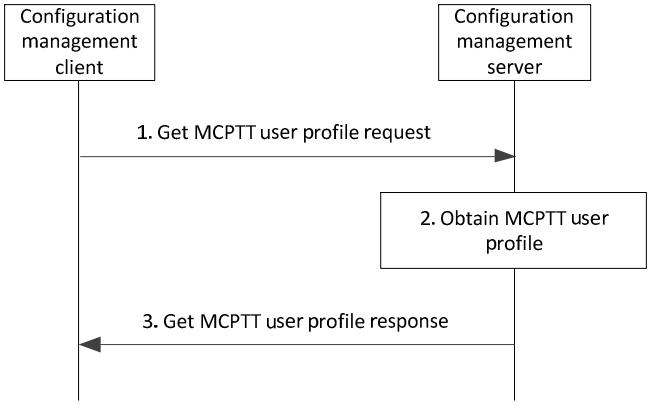

Figure 10.1.4.2-1: MCPTT user obtains the user profile (UE initiated)

1. The configuration management client sends get MCPTT user profile request message to the configuration management server. This message provides the MCPTT ID and identifies the MCPTT user profile.
2. The configuration management server obtains the MCPTT user profile information.
3. The configuration management server sends get MCPTT user profile response message to the configuration management client. When a download is necessary, this message carries the requested MCPTT user profile information that is associated with the MCPTT ID.

10.1.4.3 MCPTT user obtains the user profile update (network initiated)

The procedure for MCPTT user obtaining the user profile or an update that is initiated by network is illustrated in figure 10.1.4.3-1.

Pre-conditions:

- The MCPTT user has performed user authentication in identity management server.
- The MCPTT UE has the secure access to configuration management server.
- The configuration management server has access to the MCPTT user profile(s) associated with the MCPTT ID.

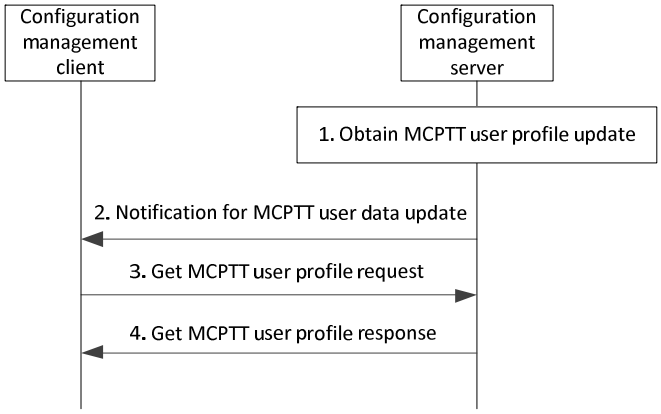

Figure 10.1.4.3-1: MCPTT user obtains the user profile update (network initiated)

1. The configuration management server obtains the MCPTT user profile update information.
2. The configuration management server sends a notification for MCPTT user data update to the configuration management client.
3. The configuration management client sends get MCPTT user profile request to the configuration management server.
4. The configuration management server sends get MCPTT user profile response to the configuration management client. This message carries the MCPTT user profile update information requested in step 3.

10.1.4.4 MCPTT user uploads the user profile data

The procedure for MCPTT user uploading the user data that is related to the MCPTT user profile is illustrated in figure 10.1.4.4-1.

Pre-conditions:

- The MCPTT user has performed user authentication in identity management server.
- The MCPTT UE has the secure access to configuration management server.

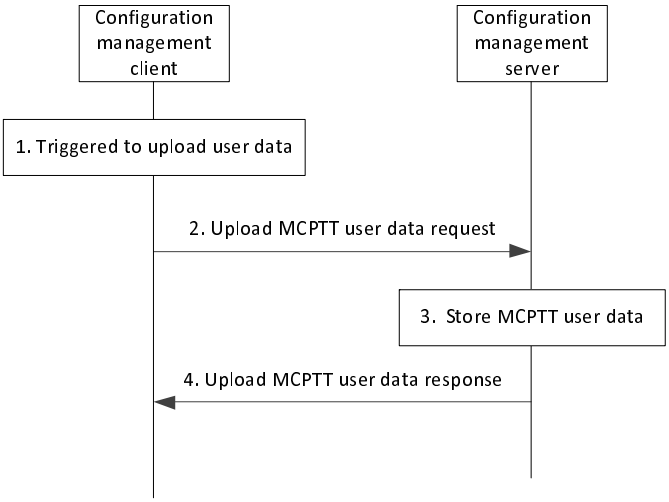

Figure 10.1.4.4-1: MCPTT user uploads the user data

1. The configuration management client is triggered (e.g. by user interaction operation or by receiving information from the configuration management server per step 2 in subclause 10.1.4.3) to upload the MCPTT user data.
2. The configuration management client sends upload MCPTT user data request to the configuration management server. The message carries the user data information to be uploaded.

3. The configuration management server stores the MCPTT user data to the database.

4. The configuration management server sends upload MCPTT user data response to configuration management client to confirm the upload is completed.

10.1.5 MCPTT group configuration management

10.1.5.1 Store group configurations at the group management server

The procedure for store group configurations at the group management server is described in figure 10.1.5.1-1.

Pre-conditions:

- The group management server may have some pre-configuration data which can be used for online group configuration validation;

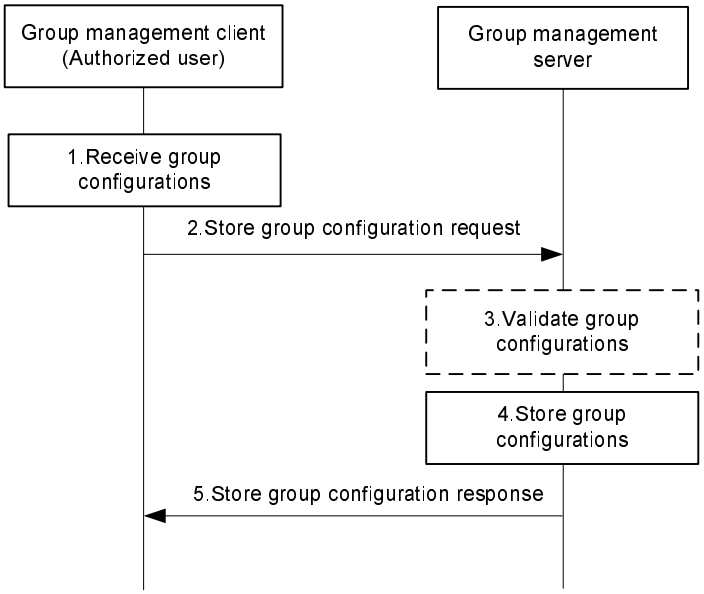

Figure 10.1.5.1-1: Store group configurations at group management server

1. The group configurations are received by the group management client of an authorized user.

2. The received group configurations are sent to the group management server for storage using a store group configuration request.

3. The group management server may validate the group configurations before storage.

4. The group management server stores the group configurations.

5. The group management server provides a store group configuration response indicating success or failure. If any validation or storage fails, the group management server provides a failure indication in the store group configuration response.

10.1.5.2 Store group configurations at the group management client

The procedure for store group configurations at the group management client is described in figure 10.1.5.2-1.

Pre-conditions:

- The group management server may have some pre-configuration data which can be used for online group configuration validation;

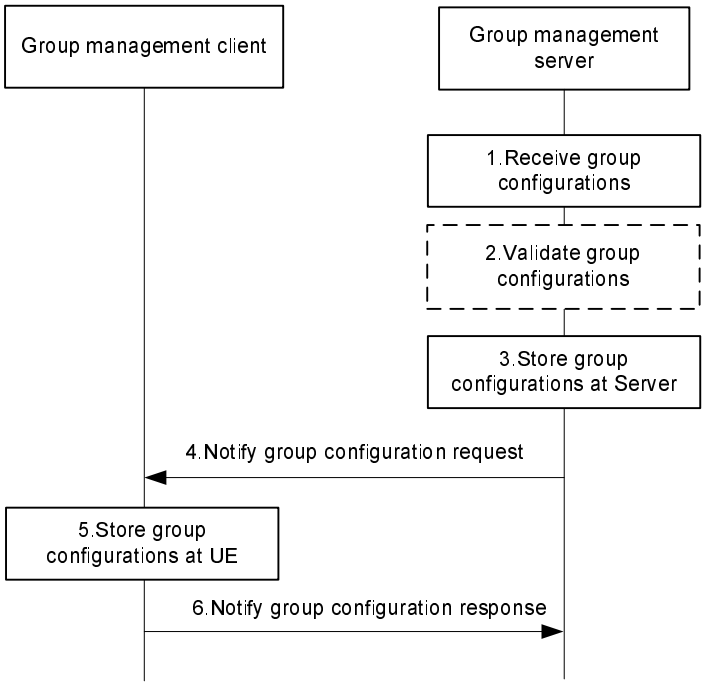

Figure 10.1.5.2-1: Store group configurations at group management client

1. The group configurations are received by the group management server.
2. The group management server may validate the group configurations before storage.
3. The group management server stores the group configurations.
4. The received group configurations are sent to the group management client for storage using a notify group configuration request.
5. The group management client stores the group configurations.
6. The group management client provides a notify group configuration response indicating success or failure.

10.1.5.3 Subscription and notification for group configuration data

The procedure for subscription for group configuration data as described in figure 10.1.5.3-1 is used by the group management client to indicate to the group management server that it wishes to receive updates of group configuration data for groups for which it is authorized.

The procedure for notification for group configuration data as described in figure 10.1.5.3-2 is used by the group management server to update the group management client with latest group configuration data.

Pre-conditions:

- The group management server has some group configurations stored.

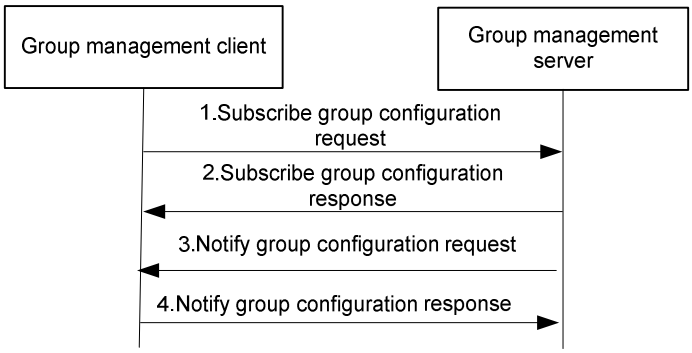

Figure 10.1.5.3-1: Subscription for group configurations

1. The group management client subscribes to the group configuration information stored at the group management server using the subscribe group configuration request.
2. The group management server provides a subscribe group configuration response to the group management client indicating success or failure of the request.
3. The notify group configuration request will provide the latest group configuration information to the group management client.
4. The group management client provides a notify group configuration response to the group management server.

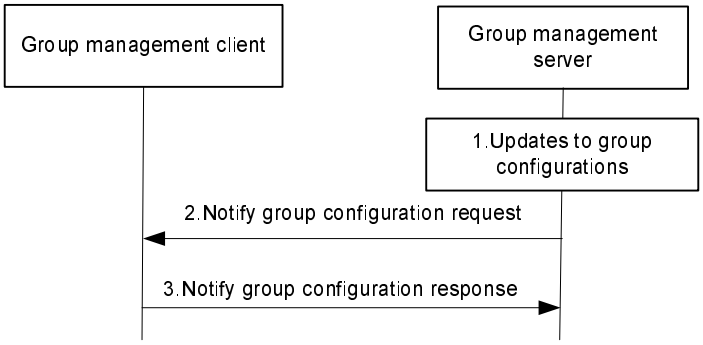

Figure 10.1.5.3-2: Notification for group configurations

1. The group management server will update the group configurations stored as a result of configuration updates for the group by administrators or authorized users.
2. The group management server provides the notification to the group management client, who previously subscribed for the group configuration information.
3. The group management client provides a notify group configuration response to the group management server.

10.1.5.4 Structure of group configuration data

The group configuration data includes the following information elements:

- MCPTT group ID;
- group owner;
- group call ongoing or not;
- group policy;
- pre-emption capability;
- pre-empted capability;

- group priority;
- associated relay service code (as specified in 3GPP TS 23.303 [8]);
- priority level of the group;
- the security level of the group;
- ProSe Layer-2 Group ID (optional) (as specified in 3GPP TS 23.303 [8]);
- ProSe Group IP multicast address (optional) (as specified in 3GPP TS 23.303 [8]); and
- indication whether the UE should use IPv4 or IPv6 for that MCPTT group (optional) (as specified in 3GPP TS 23.303 [8]).
- MCPTT ID;
- User Info Id (as specified in 3GPP TS 23.303 [8]);

NOTE 1: User Info Id is unique (identifying an MCPTT user) to enable mapping by the application from the MCPTT ID to the IP address assigned by the ProSe layer for off-network operation.

- user priority;
- participant type (first responder, second responder, dispatcher, dispatch supervisor, MCPTT administrator); and
- affiliation status.

The group configuration data also contains a set of data segments corresponding to the group whose configuration data is requested, plus all groups for which implicit affiliation is derived, i.e. group broadcast groups and group regroup groups as defined by 3GPP TS 22.179 [2].

For each data segment, the following information is provided:

- Basic status, i.e. indication on whether the group is enabled or disabled;
- Extended status, i.e. indication of potential emergency or in-peril status of the group, together with the identification of the user who has performed the last modification of this status;
- Contact URIs, i.e. additional URIs which may be used for designation of the group, for example aliases of group broadcast or group regroup group URIs;
- Media description for group media, including transport and multiplexing information; and
- Security related information, including security level.

NOTE 2: The details of security related elements are specified in 3GPP TS 33.179 [13].

10.2 User authentication for MCPTT service

NOTE: Flow 10.2-1 is a high level user authentication flow. 3GPP TS 33.179 [13] defines the specific security and authentication mechanisms required by the MCPTT service in order to realize the MCPTT user authentication requirements as defined in 3GPP TS 22.179 [2].

The user authentication process shown in flow 10.2-1 may take place in some scenarios as a separate step independently from a SIP registration phase, for example if the SIP core is outside the domain of the MCPTT server.

A possible procedure for user authentication is illustrated in figure 10.2-1. Other alternatives are possible, such as authenticating the user within the SIP registration phase.

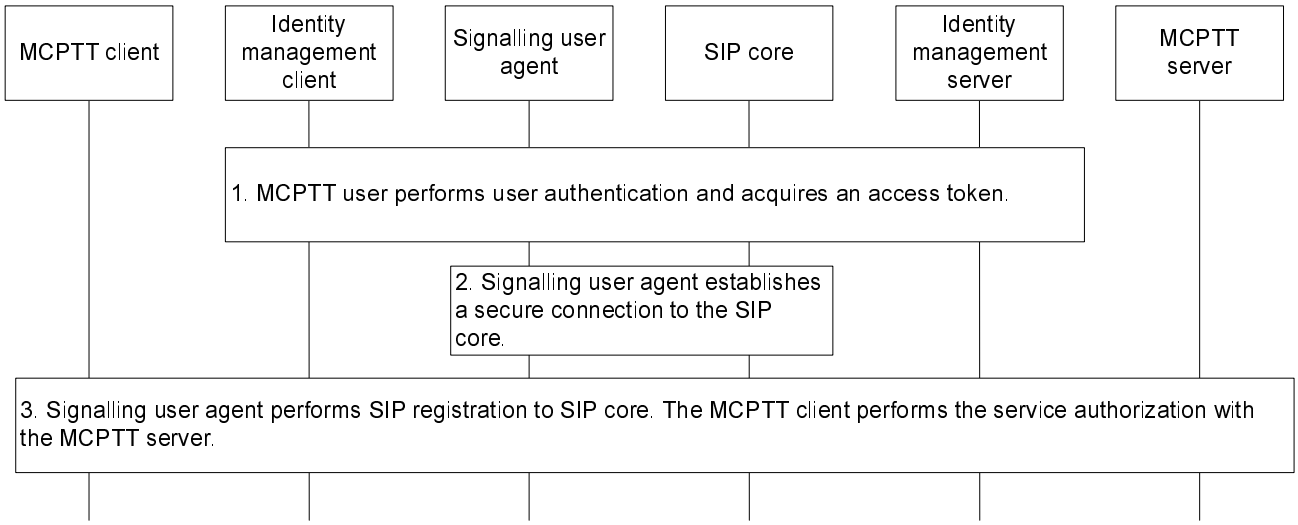

Figure 10.2-1: MCPTT user authentication and registration, single domain

1. In this optional step the identity management client begins the user authorization procedure. The MCPTT user supplies the user credentials (e.g. biometrics, secureID, username/password) for verification with the identity management server.

2. The signalling user agent establishes a secure connection to the SIP core for the purpose of SIP level authentication and registration.

3. The signalling user agent completes the SIP level registration with the SIP core (and an optional third-party registration with the MCPTT server). The MCPTT client performs the MCPTT service authorization for the user. Step 3 may utilize the results of step 1 depending on the authentication mechanism for the MCPTT user.

10.3 Affiliation to MCPTT group(s)

10.3.1 General

When an MCPTT client wants to affiliate to MCPTT group(s), it shall be subject to authorization.

10.3.2 Information flows for affiliation

10.3.2.1 MCPTT group affiliation request

Table 10.3.2.1-1 describes the information flow MCPTT group affiliation request from the MCPTT client to the MCPTT server.

Table 10.3.2.1-1: MCPTT group affiliation request

Information element	Status	Description
MCPTT ID of the originator	M	The MCPTT ID of the originator who triggers the MCPTT group affiliation request.
MCPTT group ID list	M	A list of one or more MCPTT group IDs to which the originator intents to affiliate.

10.3.2.2 MCPTT group affiliation response

Table 10.3.2.2-1 describes the information flow MCPTT group affiliation response from the MCPTT server to the MCPTT client.

Table 10.3.2.2-1: MCPTT group affiliation response

Information element	Status	Description
MCPTT ID of the originator	M	The MCPTT ID of the originator who triggers the MCPTT group affiliation request.
MCPTT group ID list	M	A list of one or more MCPTT group IDs to which the originator intents to affiliate.
Affiliation status per MCPTT group ID	M	It indicates the affiliation result for every MCPTT group ID in the list.

10.3.2.3 Group affiliation status update

Table 10.3.2.3-1 describes the information flow group affiliation status update from the MCPTT server to the group management server.

Table 10.3.2.3-1: group affiliation status update

Information element	Status	Description
MCPTT ID of the originator	M	The MCPTT ID for which the group affiliation status need to be updated.
MCPTT group ID list	M	A list of one or more MCPTT group IDs for which the affiliation status need to be updated.
Affiliation status per MCPTT group ID	M	It indicates the affiliation status for every MCPTT group ID in the list.

10.3.2.4 MCPTT group de-affiliation request

Table 10.3.2.4-1 describes the information flow MCPTT group de-affiliation request from the MCPTT client to the MCPTT server.

Table 10.3.2.4-1: MCPTT group de-affiliation request

Information element	Status	Description
MCPTT ID of the originator	M	The MCPTT ID of the originator who triggers the MCPTT group de-affiliation request.
MCPTT group ID list	M	A list of one or more MCPTT group IDs to which the originator intents to de-affiliate.

10.3.2.5 MCPTT group de-affiliation response

Table 10.3.2.5-1 describes the information flow MCPTT group de-affiliation response from the MCPTT server to the MCPTT client.

Table 10.3.2.5-1: MCPTT group de-affiliation response

Information element	Status	Description
MCPTT ID of the originator	M	The MCPTT ID of the originator who triggers the MCPTT group de-affiliation request.
MCPTT group ID list	M	A list of one or more MCPTT group IDs to which the originator intents to de-affiliate.
De-affiliation status per MCPTT group ID	M	It indicates the de-affiliation result for every MCPTT group ID in the list.

10.3.2.6 Group de-affiliation status update

Table 10.3.2.6-1 describes the information flow group de-affiliation status update from the MCPTT server to the group management server.

Table 10.3.2.6-1: group de-affiliation status update

Information element	Status	Description
MCPTT ID of the originator	M	The MCPTT ID for which the group de-affiliation status need to be updated.
MCPTT group ID list	M	A list of one or more MCPTT group IDs for which the de-affiliation status need to be updated.
De-affiliation status per MCPTT group ID	M	It indicates the de-affiliation status for every MCPTT group ID in the list.

10.3.2.7 MCPTT group affiliation change request

Table 10.3.2.7-1 describes the information flow MCPTT group affiliation change request from the MCPTT client to the MCPTT server.

Table 10.3.2.7.1: MCPTT group affiliation change request

Information element	Status	Description
MCPTT ID of the originator	M	The MCPTT ID of the originator who triggers the MCPTT group affiliation change request.
MCPTT ID list of the target user (s)	M	A list of one or more MCPTT user IDs to which the originator intend to the change their MCPTT group affiliation relationship.
MCPTT group ID list per target user	M	A list of one or more MCPTT group IDs to which the originator intents to change their affiliation relationship with the target user.
Change request type	M	It indicates the affiliation request type, i.e. mandatory or negotiated

10.3.2.8 MCPTT group affiliation change response

Table 10.3.2.8-1 describes the information flow MCPTT group affiliation change response from the MCPTT server to the MCPTT client.

Table 10.3.2.8-1: MCPTT group affiliation change response

Information element	Status	Description
MCPTT ID of the originator	M	The MCPTT ID of the originator who triggers the MCPTT group affiliation request.
MCPTT ID list of the target user (s)	M	A list of one or more MCPTT user IDs to which the originator intend to the change their MCPTT group affiliation relationship.
MCPTT group ID list	M	A list of one or more MCPTT group IDs to which the originator intents to change their affiliation relationship with the target user.
Affiliation status per MCPTT group ID	M	It indicates the affiliation relationship change result for every MCPTT group ID in the list.

10.3.3 Affiliation

10.3.3.1 MCPTT group affiliation procedure

Procedure for affiliation to MCPTT group(s) is described in figure 10.3.3.1-1.

Pre-conditions:

1. MCPTT client has already been provisioned (statically or dynamically) with the group information, or a pointer to the group information, that the MCPTT client is allowed to be affiliated.

2. MCPTT server may have retrieved the user/group policy e.g. which user(s) are authorized to affiliate to what MCPTT group(s), priority, and other configuration data.

3. MCPTT client may have indicated to the group management server that it wishes to receive updates of group configuration data for MCPTT groups(s) for which it is authorized (as described in subclause 10.1.5.3).

4. The MCPTT user triggers the affiliation procedure. This is an explicit affiliation caused by the MCPTT user.

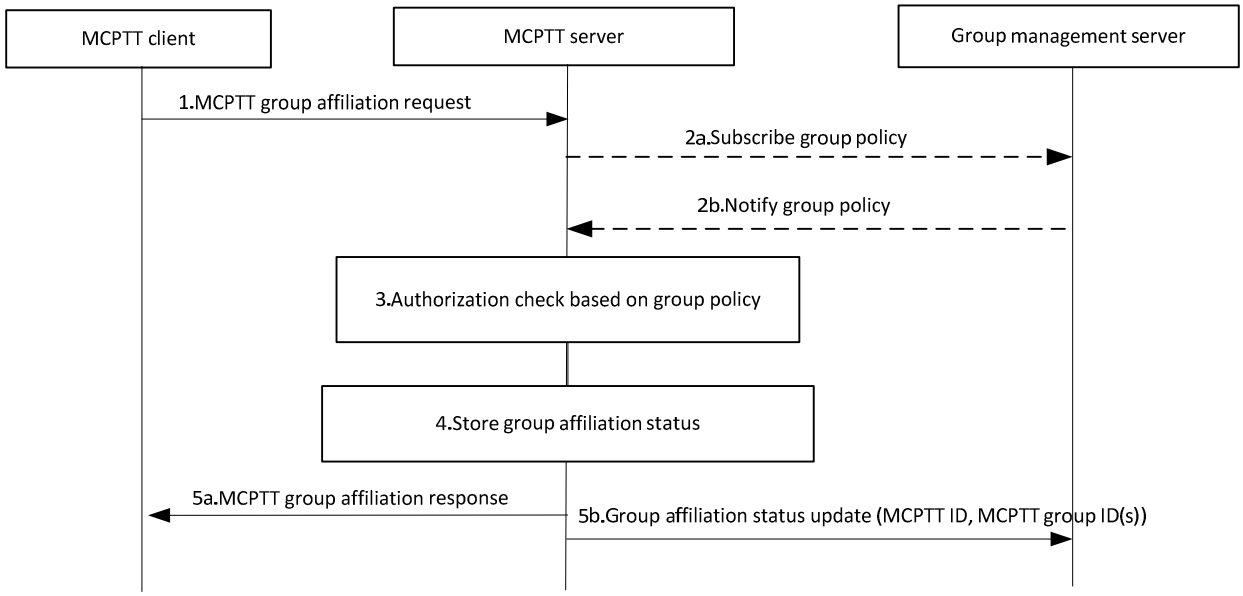

Figure 10.3.3.1-1: MCPTT group affiliation procedure

1. MCPTT client of the MCPTT user requests the MCPTT server to affiliate to an MCPTT group or a set of MCPTT groups. The MCPTT client shall provide the initiating MCPTT ID and the MCPTT group ID(s) being affiliated to.

2a. MCPTT server checks if the group policy is locally cached. If the group policy is not locally cached on the MCPTT server then MCPTT server requests the group policy from the group management server.

2b. MCPTT server receives the group policy from the group management server.

3. Based on the group policy, the MCPTT server checks if the MCPTT client is authorised to affiliate to the requested MCPTT group(s). The MCPTT server also performs the check for the maximum limit of the total number (N2) of MCPTT groups that the user can be affiliated to simultaneously.

4. If the user of the MCPTT client is authorised to affiliate to the requested MCPTT group(s) then the MCPTT server stores the affiliation status of the user for the requested MCPTT group(s).

5. MCPTT server confirms to the MCPTT client the affiliation (5a) and updates the group management server with the affiliation status of the user for the requested MCPTT group(s) (5b).

NOTE: Steps 5a and 5b can occur in any order or in parallel.

10.3.3.2 Affiliation to MCPTT group(s) defined in partner MCPTT system

10.3.3.2.1 Functional description

When an MCPTT client wants to affiliate to MCPTT group(s) which is defined in partner MCPTT system, it shall subject to authorization from the partner MCPTT system where the MCPTT group(s) is defined, and whether it subjects to authorization from the primary MCPTT system is conditional.

10.3.3.2.2 Procedure

Procedure for affiliation to MCPTT group(s) which is defined in partner MCPTT system is described in figure 10.3.3.2.2-1.

Pre-conditions:

1. The MCPTT client has already been provisioned (statically or dynamically) with the group information, or a pointer to the group information, that the MCPTT client is allowed to be affiliated.
2. The MCPTT server of the primary MCPTT system may have locally cached the MCPTT group affiliation status of the MCPTT user.
3. The MCPTT server of the partner MCPTT system may have retrieved the group related information from the group management server.
4. The MCPTT client may have indicated to the group management server of the partner MCPTT system that it wishes to receive updates of group configuration data for MCPTT group(s) for which it is authorized (as described in subclause 10.1.5.3).
5. The MCPTT user triggers the affiliation procedure. This is an explicit affiliation caused by the MCPTT user.

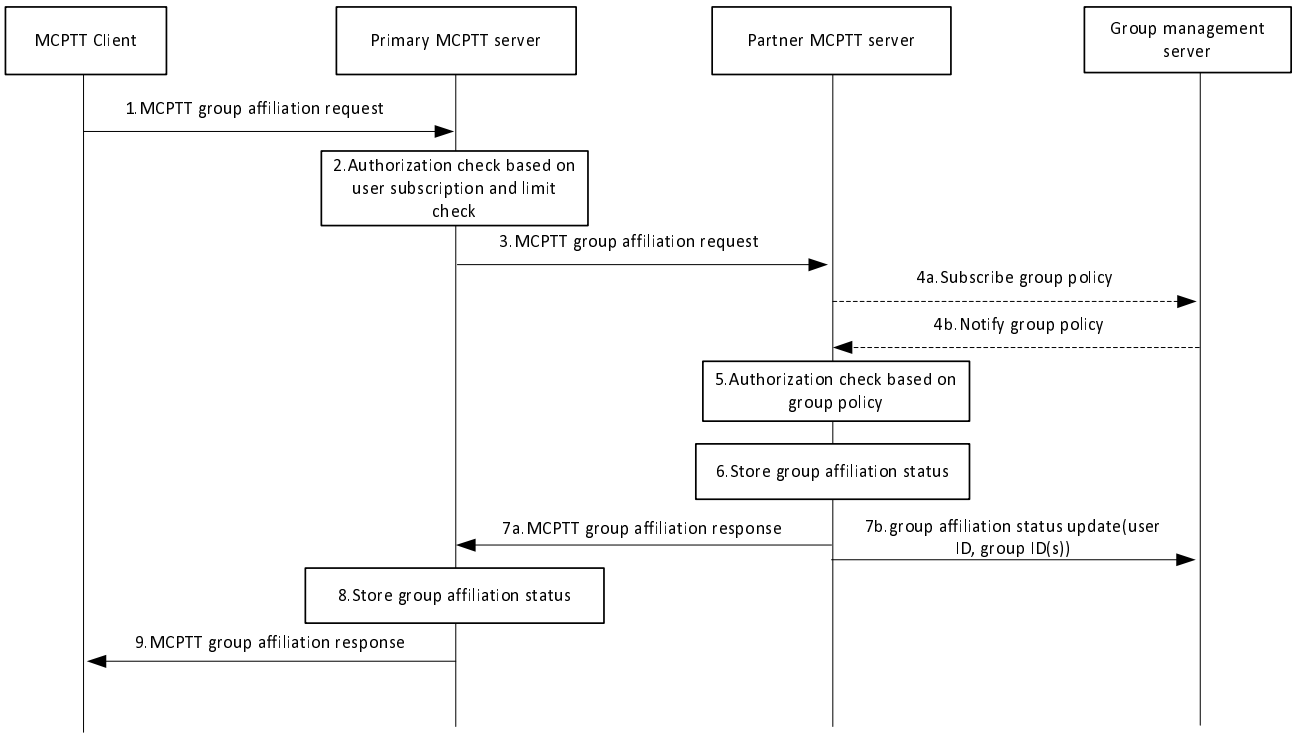

Figure 10.3.3.2.2-1: Affiliation for an MCPTT group defined in partner MCPTT system

1. The MCPTT client requests the MCPTT server of the primary MCPTT system to affiliate to an MCPTT group or a set of MCPTT groups. The MCPTT client shall provide the initiating user ID and the MCPTT group ID(s) being affiliated to.
2. The MCPTT server of the primary MCPTT system shall check if the MCPTT client is authorized to affiliate to the requested MCPTT group(s) based on the user subscription. The MCPTT server also performs the check for the maximum limit of the total number (N2) of MCPTT groups that the user can be affiliated to simultaneously.
3. Based on the group information included in the request, the MCPTT server of the primary MCPTT system, it determines to send group affiliation request to the corresponding MCPTT server of the partner MCPTT system. The request may be routed through some intermediate signalling nodes.

4a. The MCPTT server of the partner MCPTT system checks if the group policy is locally cached. If the group policy is not locally cached on the MCPTT server then MCPTT server subscribes to the group policy from the group management server.

4b. The MCPTT server of the partner MCPTT system receives the group policy from the group management server via notification and locally caches the group policy information.

5. Based on the group policy, the MCPTT server of the partner MCPTT system checks if the MCPTT group(s) is not disabled and if the user of the MCPTT client is authorised to affiliate to the requested MCPTT group(s).

6. If the user of the MCPTT client is authorised to affiliate to the requested MCPTT group(s) then the MCPTT server of the partner MCPTT system stores the affiliation status of the user for the requested MCPTT group(s).

7. The MCPTT server of the partner MCPTT system sends the affiliation status result of requested MCPTT group(s) to the MCPTT server of the primary MCPTT system (7a) and updates the group management server with the affiliation status of the user for the requested MCPTT group(s) (7b).

NOTE: Steps 7a and 7b can occur in any order or in parallel.

8. The MCPTT server of the primary MCPTT system stores the affiliation status of the user for the requested MCPTT group(s).

9. The MCPTT server of the primary MCPTT system sends the group affiliation status result for the requested MCPTT group(s) to the MCPTT client.

10.3.4 De-affiliation from MCPTT group(s)

10.3.4.1 General

When an MCPTT user does not want to communicate with an MCPTT group anymore, the MCPTT user can revoke its affiliation to the MCPTT group.

10.3.4.2 MCPTT group de-affiliation procedure

Procedure for revoking the affiliation with an MCPTT group is described in figure 10.3.4.2-1.

Pre-conditions:

1. MCPTT server has already subscribed to the MCPTT group information from group management server and has stored the data of MCPTT group(s) to which the MCPTT user is affiliated to.

2. The MCPTT user triggers the de-affiliation procedure.

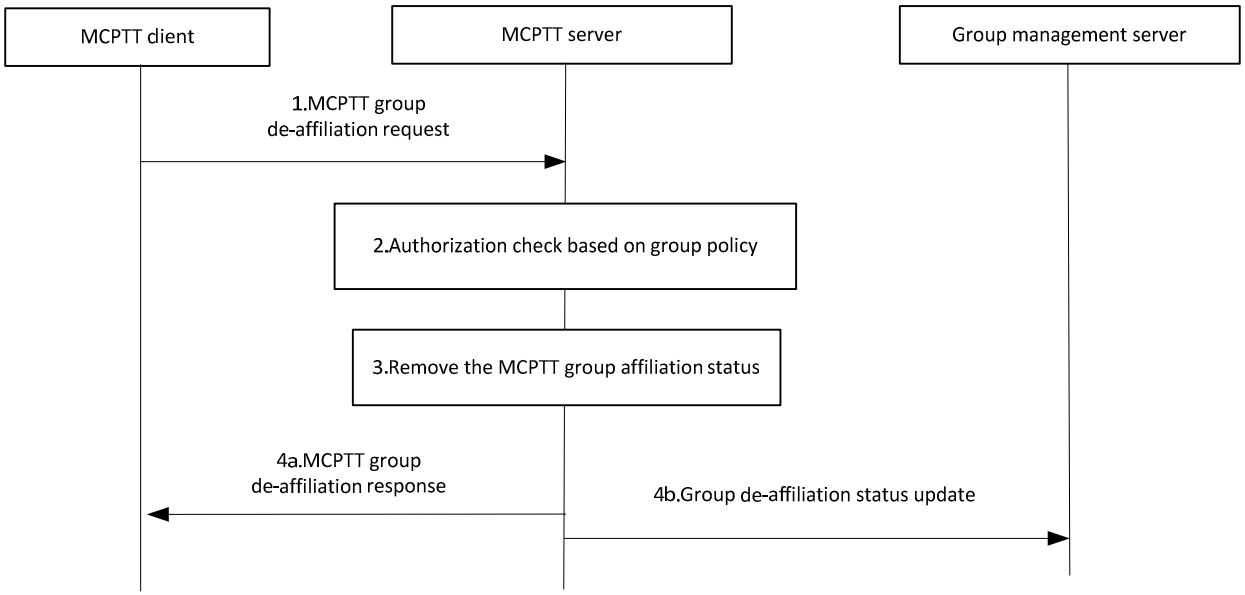

Figure 10.3.4.2-1: MCPTT group de-affiliation procedure

1. MCPTT client requests the MCPTT server to de-affiliate to an MCPTT group or set of MCPTT groups.
2. Based on the stored group policy, the MCPTT server checks if the MCPTT client is authorized to de-affiliate to the requested MCPTT group(s).
3. If the user of the MCPTT client is authorized to de-affiliate to the requested MCPTT group(s) then the MCPTT server removes the affiliation status of the user for the requested MCPTT group(s).
4. MCPTT server provides to the MCPTT client with the group de-affiliation response (4a) and updates the group management server with the de-affiliation status of the user for the requested MCPTT group(s) (4b).

NOTE: Steps 4a and 4b can occur in any order or in parallel.

10.3.4.3 De-affiliation from MCPTT group(s) defined in partner MCPTT system

Procedure for de-affiliation from affiliated MCPTT group(s) which is defined in partner MCPTT system is described in figure 10.3.4.3-1.

Pre-conditions:

1. The primary/partner MCPTT servers have already subscribed to the group information from group management server and stored the data of MCPTT group(s) to which the MCPTT user intends to de-affiliate.

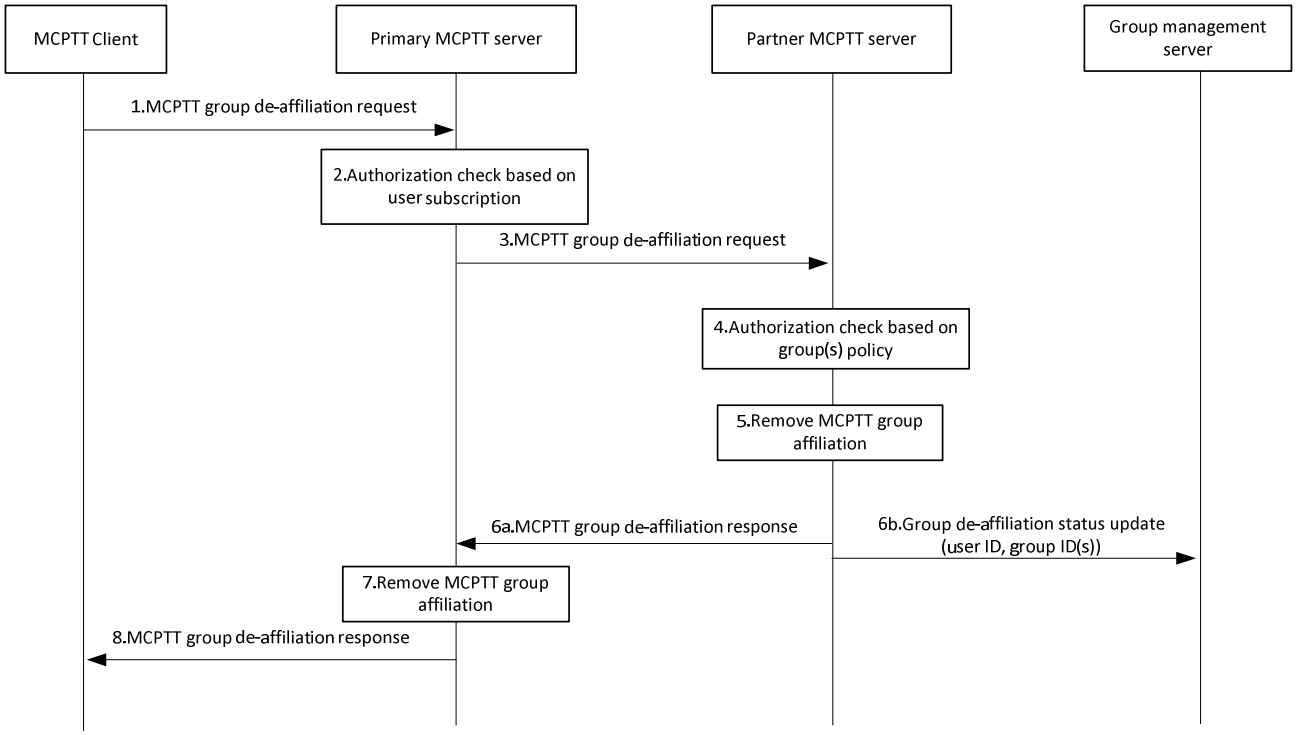

Figure 10.3.4.3-1: De-affiliation from an MCPTT group defined in partner MCPTT system

1. The MCPTT client requests the primary MCPTT server to de-affiliate to an MCPTT group or a set of MCPTT groups.

2. The primary MCPTT server shall check if the MCPTT client is authorized to de-affiliate to the requested MCPTT group(s) based on the user subscription. The primary MCPTT server performs the check if the user has affiliated to the MCPTT groups.

3. Based on the MCPTT group information included in the request, the primary MCPTT server determines to send MCPTT group de-affiliation request to the corresponding partner MCPTT server. The request may be routed through some intermediate signalling nodes.

4. Based on the stored group policy, the partner MCPTT server checks if the MCPTT group is not disabled and if the user of the MCPTT client has affiliated to the requested MCPTT group(s) and is authorized to de-affiliate to the requested MCPTT group(s).

5. If the user of the MCPTT client has affiliated to the requested MCPTT group(s) and is authorized to de-affiliate to the requested MCPTT group(s), then the partner MCPTT server removes the affiliation status of the user for the requested MCPTT group(s).

6. The partner MCPTT server sends the MCPTT group de-affiliation response to primary MCPTT server (6a) and updates the group management server with the de-affiliation status of the user for the requested MCPTT group(s) (6b).

NOTE: Steps 6a and 6b can occur in any order or in parallel.

7. The primary MCPTT server will remove any information stored about the user's affiliation with requested MCPTT group(s) of partner MCPTT system.

8. The primary MCPTT server sends the MCPTT group de-affiliation response to the MCPTT client.

10.3.5 Remote change of affiliation

10.3.5.1 Remote change of affiliation for groups defined in primary MCPTT system

10.3.5.1.1 Authorized user remotely changes another MCPTT user's affiliated MCPTT group(s) – mandatory mode

Procedure for the authorized user to remotely change another MCPTT user's affiliated MCPTT group(s) without requiring target user's approval is described in figure 10.3.5.1.1-1.

Pre-conditions:

- The MCPTT client 1 (authorized user) has already been provisioned (statically or dynamically) with the target MCPTT user's information and its group information, that target MCPTT user 2 is allowed to be affiliated;
- The primary MCPTT server may have retrieved the user/group policy e.g. information regarding user(s) authorization to affiliate to MCPTT group(s), priority, and other related meta-data.

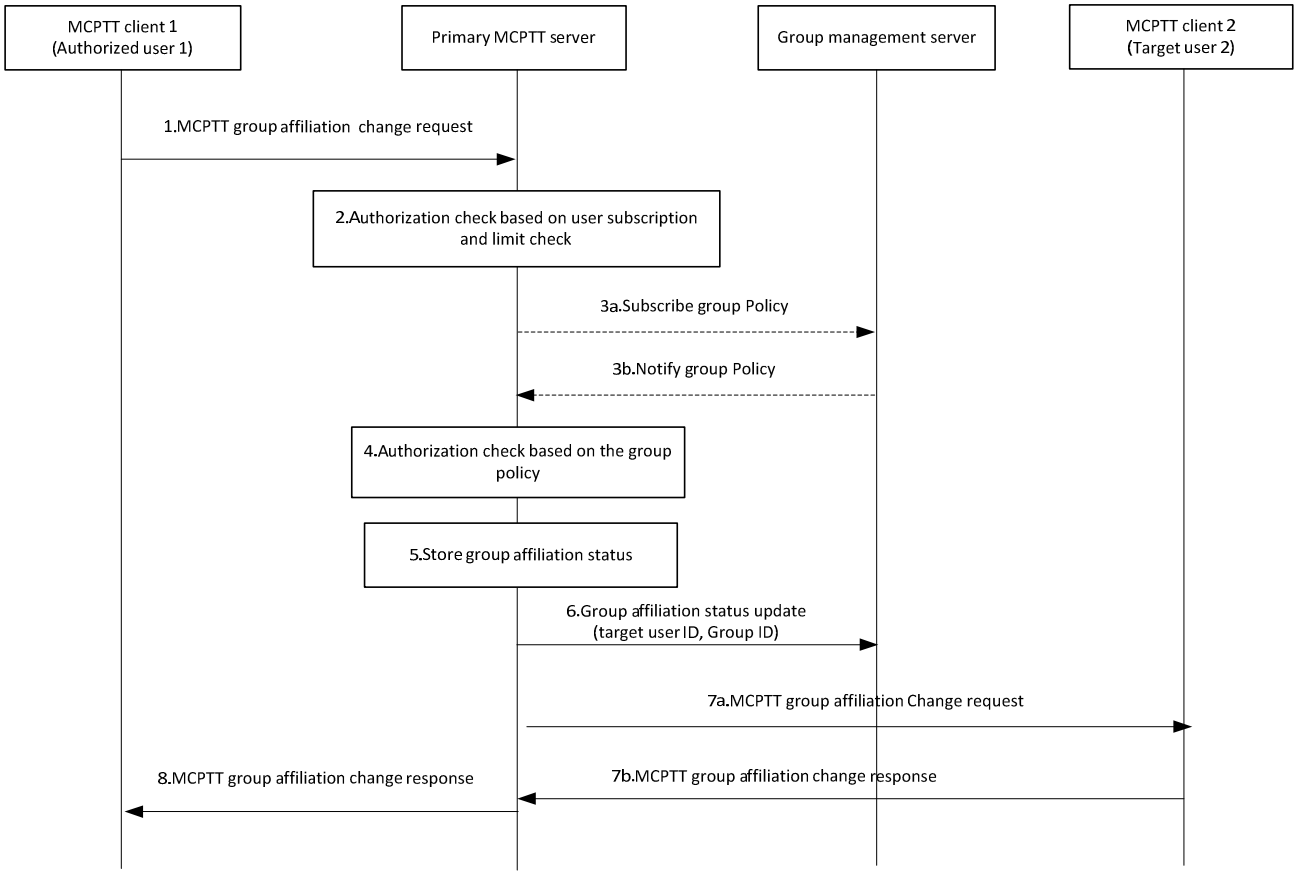

Figure 10.3.5.1.1-1: Remotely change MCPTT group affiliation – mandatory mode

1. When an authorized user requires one or more MCPTT users to change the affiliation to an MCPTT group or set of MCPTT groups, the MCPTT client 1 of the authorized user 1 sends MCPTT group affiliation change request with the indication of mandatory mode to the primary MCPTT server. The information (i.e. target MCPTT user(s) ID, MCPTT group(s) ID) used to indicate the change of the affiliation relationship between the target MCPTT user 2 and the MCPTT group(s) shall be included.
2. The primary MCPTT server shall check if the MCPTT user 1 is authorized to initiate the change of the affiliation relationship between the target user 2 and the MCPTT group(s). The primary MCPTT server shall check if the target MCPTT user(s) are authorized for the requested affiliation relationship based on the user subscription. The primary MCPTT server also performs the check for the maximum limit on the total number (N2) of MCPTT groups that the user can be affiliated to simultaneously.

3a. The primary MCPTT server checks if the group policy is locally cached. If the group policy is not locally cached on the MCPTT server, then, the MCPTT server subscribes to the group policy from the group management server.

3b. The primary MCPTT server receives the group policy from the group management server via notification and locally caches the group policy information.

4. Based on the group policy, the primary MCPTT server checks if the target MCPTT user 2 is authorized to affiliate or de-affiliate to the MCPTT group(s). It is possible that the target MCPTT user 2 affiliates to one or several MCPTT groups and also de-affiliates from one or more MCPTT groups.

5. If the target MCPTT user 2 is authorized to affiliate or de-affiliate to the MCPTT group(s) then the primary MCPTT server stores the new affiliation status of the target MCPTT user 2 for the MCPTT group(s).

6. The primary MCPTT server updates the group management server with the affiliation status of the MCPTT user 2 for the MCPTT group(s).

7a. The primary MCPTT server sends the MCPTT group affiliation change request with the indication of mandatory mode to MCPTT client 2 of the target MCPTT user 2. The target MCPTT user 2 receives the latest information about the affiliated MCPTT groups. Further the MCPTT client 2 may subscribe for the affiliated MCPTT groups information with the group management server.

7b. If the target MCPTT user 2 provides a response to the primary MCPTT server.

8. The primary MCPTT server sends the MCPTT group affiliation change response to MCPTT client 1.

NOTE: Steps 6, 7 and 8 can occur in any order or in parallel.

10.3.5.1.2 Authorized user remotely changes another MCPTT user's affiliated MCPTT group(s) – negotiated mode

Procedure for the authorized user to remotely change another MCPTT user's affiliated MCPTT group(s) with the target MCPTT user's approval is described in figure 10.3.5.1.2-1.

Pre-conditions:

- The MCPTT client has already been provisioned (statically or dynamically) with target MCPTT user's information and its group information, that target user's MCPTT client is allowed to be affiliated;

- The primary MCPTT server may have retrieved the user/group policy e.g. information regarding user(s) authorization to affiliate to MCPTT group(s), priority, and other related meta-data.

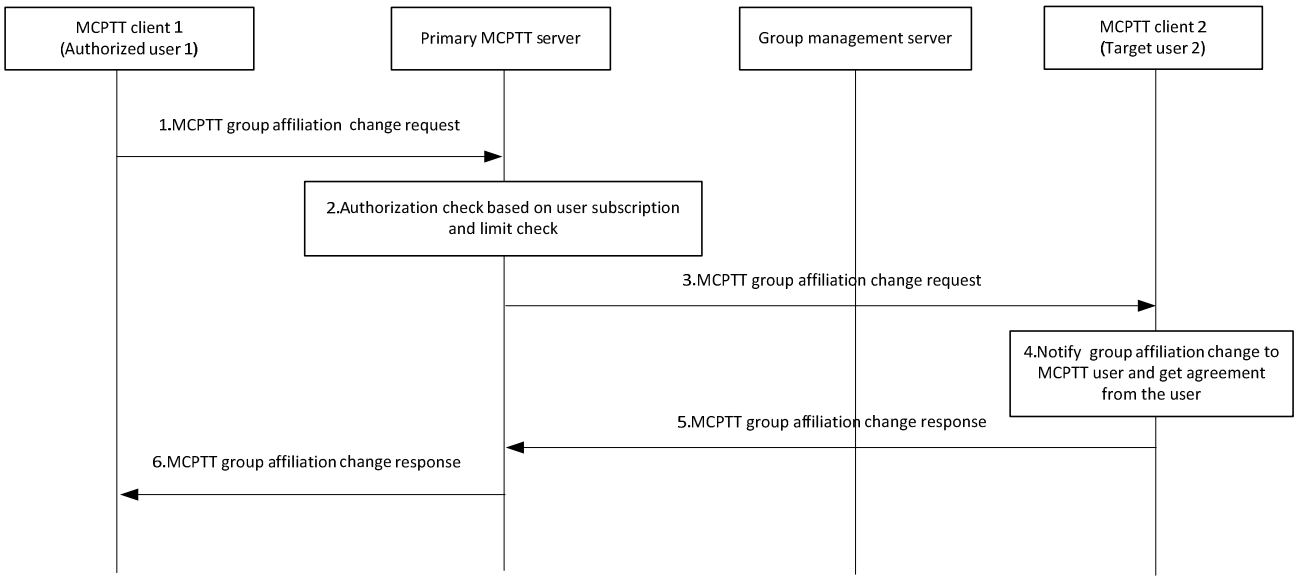

Figure 10.3.5.1.2-1: Remotely change MCPTT group affiliation – negotiated mode

1. When an authorized user requires one or more MCPTT users to change the affiliation to an MCPTT group or set of MCPTT groups, the MCPTT client 1 of the authorized user 1 sends MCPTT group affiliation change request to the primary MCPTT server. The information (i.e. target MCPTT user(s) ID, MCPTT group(s) ID) used to indicate the change of the affiliation relationship between the target MCPTT user 2 and the MCPTT group(s) shall be included.

2. The primary MCPTT server shall check if the MCPTT user 1 is authorized to initiate the change of the affiliation relationship between the target user 2 and the MCPTT group(s). The primary MCPTT server shall check if the target MCPTT user(s) are authorized for the requested affiliation relationship based on the user subscription. The primary MCPTT server also performs the check for the maximum limit on the total number (N2) of MCPTT groups that the user can be affiliated to simultaneously.

3. If the target MCPTT user 2 is authorized to the changes to its affiliated MCPTT group(s), the primary MCPTT server sends the MCPTT group affiliation change request to the MCPTT client 2 of the target MCPTT user 2.

4. The MCPTT client 2 notifies the MCPTT group affiliation change request to the target MCPTT user 2 to receive the approval from the user on the proposed changes to the affiliated MCPTT group(s).

NOTE 1: The procedure is aborted if the target MCPTT user 2 does not respond to the notification within an implementation dependent time.

5. If the target MCPTT user 2 provides a response (accept or reject) to the notification, then the MCPTT client 2 sends an MCPTT group affiliation change response to the primary MCPTT server. An response indicating target user 2's acceptance to the requested affiliation change by authorized user 1, triggers the affiliation or de-affiliation procedures at the primary MCPTT server (see subclause 10.3) as per the MCPTT user 1's requested changes to the target user 2's affiliated group(s).

NOTE 2: In the case where the affiliation changes for target user 2 includes MCPTT groups defined in partner MCPTT systems, the primary MCPTT server performs the affiliation or de-affiliation procedures by interacting with the partner MCPTT systems (see subclause 10.3).

6. The primary MCPTT server sends the MCPTT group affiliation change response to the MCPTT client 1.

If multiple MCPTT groups are included in step 1, and these MCPTT groups belong to different partner MCPTT systems, the primary MCPTT server may wait until all the partner MCPTT systems provides the MCPTT group affiliation change response messages.

10.3.5.2 Remote change of affiliation for groups defined in partner MCPTT system

10.3.5.2.1 Authorized user remotely changes another MCPTT user's affiliated MCPTT group(s) defined in partner MCPTT system – mandatory mode

Procedure for the authorized user to remotely change another MCPTT user's affiliated MCPTT group(s) defined in partner MCPTT systems without requiring target user's approval is described in figure 10.3.5.2.1-1.

Pre-conditions:

- The MCPTT client 1 (authorized user) has already been provisioned (statically or dynamically) with the target MCPTT user 2's information and group information, that the target MCPTT user 2 is allowed to be affiliated;

- The partner MCPTT server may have retrieved the group related information from the group management server;

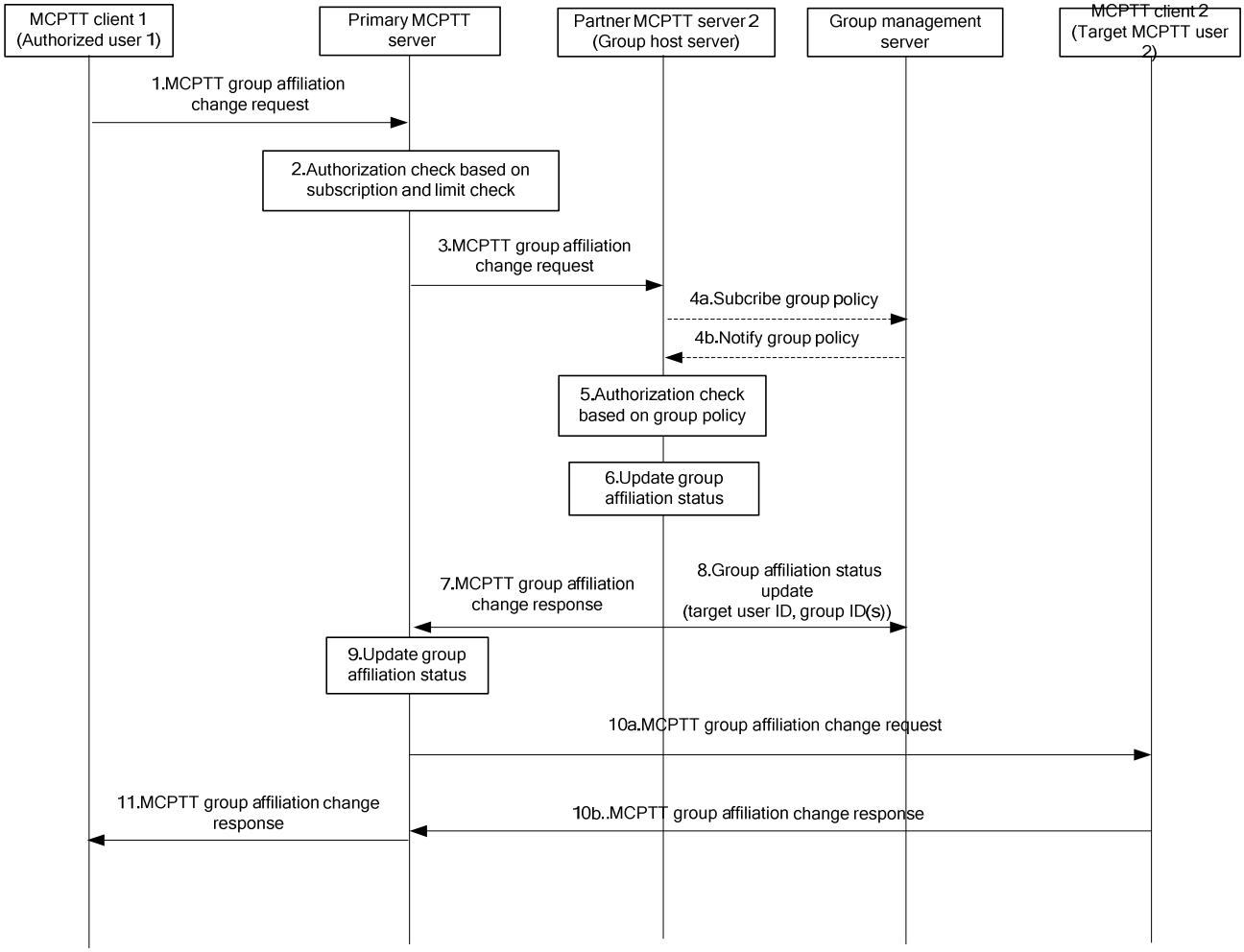

Figure 10.3.5.2.1-1: Remote change MCPTT group affiliation defined in partner MCPTT system – mandatory mode

1. When an authorized user requires one or more MCPTT users to change the affiliation to an MCPTT group or set of MCPTT groups, the MCPTT client 1 of the authorized user 1 sends MCPTT group affiliation change request with the indication of mandatory mode to the primary MCPTT server. The information (i.e. target MCPTT user(s) ID, MCPTT group(s) ID) used to indicate the change of the affiliation relationship between the target MCPTT user 2 and the MCPTT group(s) shall be included.

2. The primary MCPTT server shall check if the MCPTT user 1 is authorized to initiate the change of the affiliation relationship between the target user 2 and the MCPTT group(s). The primary MCPTT server shall check if the target MCPTT user(s) are authorized for the requested affiliation relationship based on the user subscription. The primary MCPTT server also performs the check for the maximum limit on the total number (N2) of MCPTT groups that the user can be affiliated to simultaneously.

3. Based on the MCPTT group information included in the request, the primary MCPTT server determines to send MCPTT group affiliation change request to the corresponding partner MCPTT server (group host server).

4a. The partner MCPTT server checks if the group policy is locally cached. If the group policy is not locally cached on the partner MCPTT server then the partner MCPTT server subscribes to the group policy from the group management server.

4b. The partner MCPTT server receives the group policy from the group management server via notification and locally caches the group policy information.

5. Based on the group policy, the partner MCPTT server checks if the target MCPTT user 2 is authorized to affiliate to the MCPTT group(s). It is possible that the target MCPTT user 2 affiliates to one or several MCPTT groups and also de-affiliates from one or more MCPTT groups.

6. If the target MCPTT user 2 is authorized to affiliate or de-affiliate to the MCPTT group(s), then the partner MCPTT server stores the new affiliation status of the target MCPTT user 2 for the MCPTT group(s).

7. The partner MCPTT server updates the group management server with the affiliation status of the target MCPTT user 2 for the MCPTT group(s).

8. The partner MCPTT server sends the MCPTT group affiliation change response to the primary MCPTT server.

9. The primary MCPTT server stores the new affiliation status of the target MCPTT user 2 for the MCPTT group(s).

NOTE: Steps 8 and 9 can occur in any order or in parallel.

10a. The primary MCPTT server sends the MCPTT group affiliation change request with the indication of mandatory mode to MCPTT client 2 of the target MCPTT user 2. The target MCPTT user 2 receives the latest information about the affiliated MCPTT groups. Further the MCPTT client 2 may subscribe for the affiliated MCPTT groups information with the group management server.

10b. The target MCPTT user 2 provides an MCPTT group affiliation change response to the MCPTT server.

11. The primary MCPTT server sends the MCPTT group affiliation change response to MCPTT client 1 (authorized user).

10.4 Group management (on-network)

10.4.1 General

Group management procedures apply to on-network MCPTT service only.

Group creation provides a dedicated MCPTT group to individual MCPTT users to enable the required communication. This includes the normal group creation by administrators as well as user regrouping by authorized user/dispatcher.

Group regrouping enables dispatchers or authorized users to temporarily combine different MCPTT groups.

10.4.2 Information flows for group management

10.4.2.1 Group creation request

Table 10.4.2.1-1 describes the information flow group creation request from the group management client to the group management server.

Table 10.4.2.1-1: Group creation request

Information element	Status	Description
MCPTT ID list	M	List of MCPTT IDs that are part of the group to be created

10.4.2.2 Group creation confirmation response

Table 10.4.2.2-1 describes the information flow group creation confirmation response from the group management server to the group management client.

Table 10.4.2.2-1: Group creation confirmation response

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the group

10.4.2.3 Group regroup request

Table 10.4.2.3-1 describes the information flow group regroup request from the group management client to the group management server.

Table 10.4.2.3-1: Group regroup request

Information element	Status	Description
MCPTT group ID list	M	List of MCPTT group IDs to be combined
Security level	O	Required security level for the temporary group
Priority level	O	Required priority level for the temporary group

10.4.2.4 Group regroup confirmation response

Table 10.4.2.4-1 describes the information flow group regroup confirmation response from the group management server to the group management client.

Table 10.4.2.4-1: Group regroup confirmation response

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the temporary group
Result	M	Indicates the success or failure of group regroup

10.4.2.5 Group regroup teardown request

Table 10.4.2.5-1 describes the information flow group regroup teardown request from the group management client to the group management server.

Table 10.4.2.5-1: Group regroup teardown request

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the temporary group which is requested to be torn down

10.4.2.6 Group regroup teardown response

Table 10.4.2.6-1 describes the information flow group regroup teardown response from the group management server to the group management client.

Table 10.4.2.6-1: Group regroup teardown response

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the temporary group
Result	M	Indicates the success or failure of group regroup teardown

10.4.2.7 Group creation notify

Table 10.4.2.7-1 describes the information flow group creation notify from the group management server to the MCPTT server.

Table 10.4.2.7-1: Group creation notify

Information element	Status	Description
MCPTT ID list	M	List of MCPTT IDs that are part of the created group

10.4.2.8 Group regroup notify

Table 10.4.2.8-1 describes the information flow group regroup notify from the group management server to the MCPTT server.

Table 10.4.2.8-1: Group regroup notify

Information element	Status	Description
MCPTT group ID list	M	List of constituent MCPTT group IDs
MCPTT group ID	M	MCPTT group ID of the temporary group

10.4.2.9 Group regroup teardown notify

Table 10.4.2.9-1 describes the information flow group regroup teardown notify from the group management server to the MCPTT server.

Table 10.4.2.9-1: Group regroup teardown notify

Information element	Status	Description
MCPTT group ID	M	MCPTT group ID of the temporary group which is being torn down

10.4.2.10 Group regroup request

Table 10.4.2.10-1 describes the information flow group regroup request between group management servers.

Table 10.4.2.10-1: Group regroup request

Information element	Status	Description
MCPTT group ID list	M	List of constituent MCPTT group IDs belonging to the target group management server

10.4.2.11 Group regroup response

Table 10.4.2.11-1 describes the information flow group regroup response between group management servers.

Table 10.4.2.11-1: Group regroup response

Information element	Status	Description
Result	M	Indicates whether the group regroup was accepted or rejected by the group management server in the partner system
MCPTT group ID list	O	List of constituent MCPTT group IDs from group management server of the partner system which are being combined into the temporary group

10.4.2.12 Group regroup notification

Table 10.4.2.12-1 describes the information flow group regroup notification between group management servers.

Table 10.4.2.12-1: Group regroup notification

Information element	Status	Description
MCPTT group ID list	M	List of constituent MCPTT group IDs
MCPTT group ID	M	MCPTT group ID of the temporary group
Priority level	O	Required priority level for the temporary group
Security level	O	Required security level for the temporary group

10.4.2.13 Group regroup notification response

Table 10.4.2.13-1 describes the information flow group regroup notification response between group management servers.

Table 10.4.2.13-1: Group regroup notification response

Information element	Status	Description
MCPTT group ID list	M	List of constituent MCPTT group IDs
MCPTT group ID	M	MCPTT group ID of the temporary group
Priority level	O	Required priority level for the temporary group
Security level	O	Required security level for the temporary group

10.4.3 Group creation

Figure 10.4.3-1 below illustrates the group creation operations by authorized MCPTT user/MCPTT administrator to create a group. It applies to the scenario of normal group creation by an MCPTT administrator and user regrouping operations by authorized user/dispatcher.

Pre-conditions:

1. The group management client, group management server, MCPTT server and the MCPTT group members belong to the same MCPTT system.

2. The administrator/authorized user/dispatcher is aware of the users' identities which will be combined to form the MCPTT group.

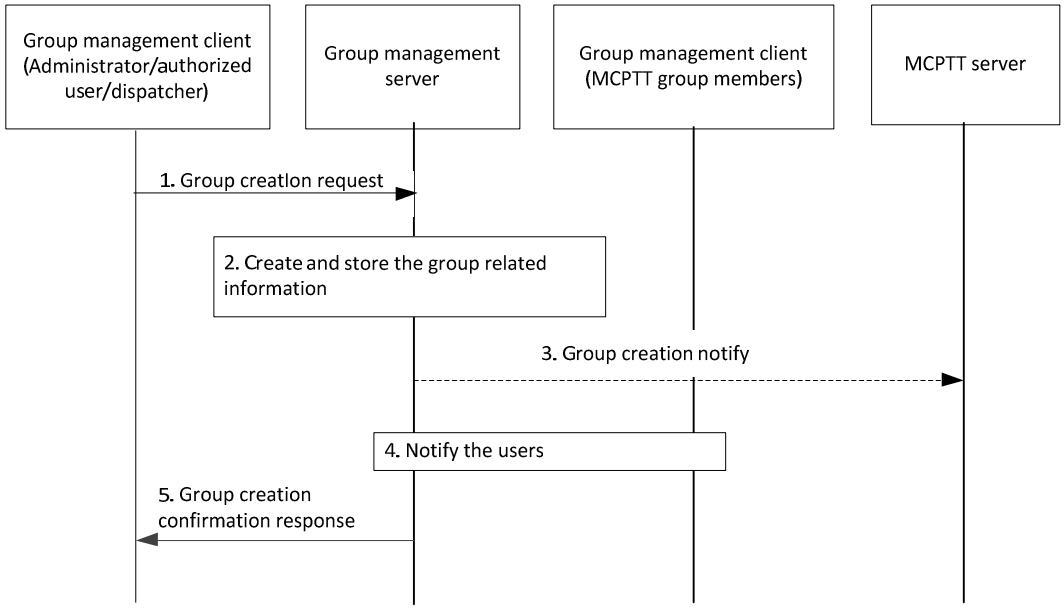

Figure 10.4.3-1: Group creation

1. The group management client of the administrator/dispatcher/authorized MCPTT user requests group create operation to the group management server. The identities of the users being combined shall be included in this message.

2. During the group creation, the group management server creates and stores the information of the group as group configuration data as described in subclause 10.1.5.4. The group management server performs the check on the maximum limit of the total number (N11) of MCPTT group members for the MCPTT group(s).

3. The group management server may conditionally notify the MCPTT server regarding the group creation with the information of the group members. During user regroup, the group management server notifies the MCPTT server regarding the group creation with the information of the temporary group members. The MCPTT users of the temporary group may be automatically affiliated, if configured on the MCPTT server.

4. The MCPTT group members of the MCPTT group are notified about the newly created MCPTT group configuration data.

5. The group management server provides a group creation confirmation response to the group management client of the administrator/dispatcher/authorized MCPTT user.

10.4.4 Group regrouping

10.4.4.1 Temporary group formation - group regrouping within an MCPTT system

Figure 10.4.4.1-1 below illustrates the group regroup operations to create a temporary group within an MCPTT system. For simplicity, only the case of two MCPTT groups being combined is represented, but the procedure is the same if more than two groups are combined.

Pre-conditions:

1. The group management client, group management server, MCPTT server and the MCPTT group members belong to the same MCPTT system.

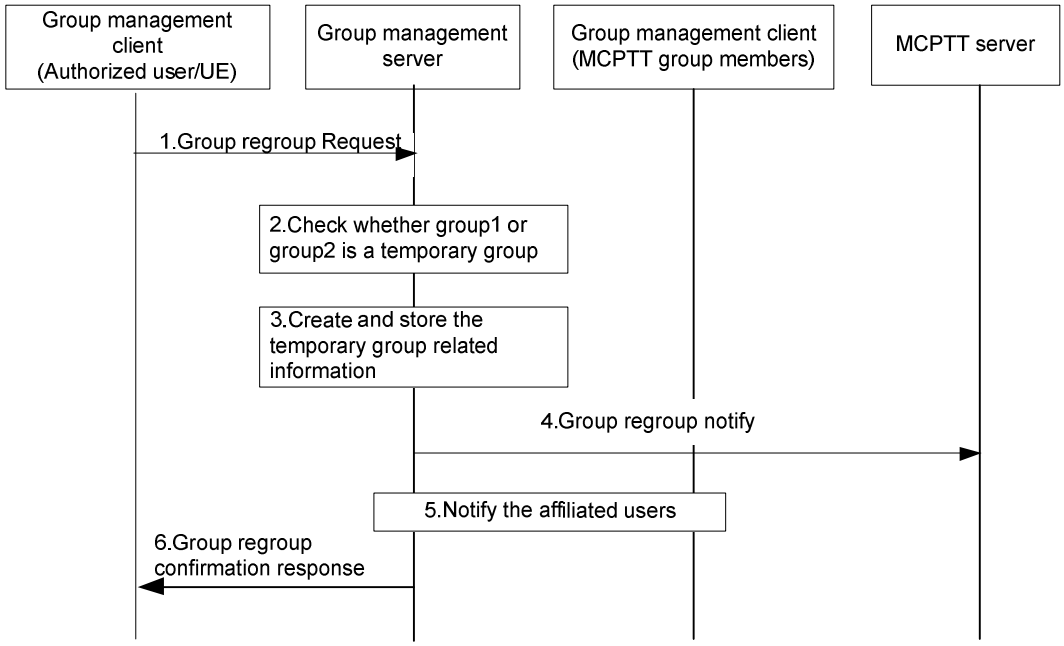

Figure 10.4.4.1-1: Group regroup for the groups within the same MCPTT system

1. The group management client of the authorized MCPTT user requests group regroup operation to the group management server, where the groups being combined are within the same MCPTT system. The identities of the groups being combined shall be included in this message. The group management client may indicate the security level required for the temporary group. The group management client may indicate the priority level required for the temporary group.

2. The group management server checks whether group1 or group2 is a temporary group. If group 1 or group2 is a temporary group, then the group regrouping will be rejected, otherwise the group regrouping can proceed.

3. The group management server creates and stores the information of the temporary group, including the temporary group identity, the identities of the groups being combined, the priority level of the temporary group and the security level of the temporary group. If the authorized MCPTT user does not specify the security level

and the priority level, the group management server shall set the lowest security level and the highest priority of the constituent groups.

4. The group management server notifies the MCPTT server regarding the temporary group creation with the information of the constituent groups, i.e. temporary group id, group1 id and group2 id.

5. The group management server notifies the affiliated MCPTT group members of the constituent MCPTT groups, possibly with an indication of lower security level.

6. The group management server provides a group regroup confirmation response to the group management client of the dispatcher/authorized MCPTT user.

10.4.4.2 Temporary group formation involving multiple MCPTT systems

Figure 10.4.4.2-1 below illustrates the group regroup operations to create a temporary group involving multiple MCPTT systems. For simplicity, only the case of two MCPTT groups being combined is represented, but the procedure is the same if more than two groups are combined.

Pre-conditions:

1. The security aspects of sharing the user information between primary and partner MCPTT systems shall be governed as per the service provider agreement between them. In this case, we consider the partner MCPTT system does not share their users' information to the primary MCPTT system.

2. The primary MCPTT system consists of the group management server 1 and MCPTT server (primary). The partner MCPTT system consists of the group management server 2 and MCPTT server (partner).

3. The group management client of the authorized MCPTT user belongs to the primary MCPTT system.

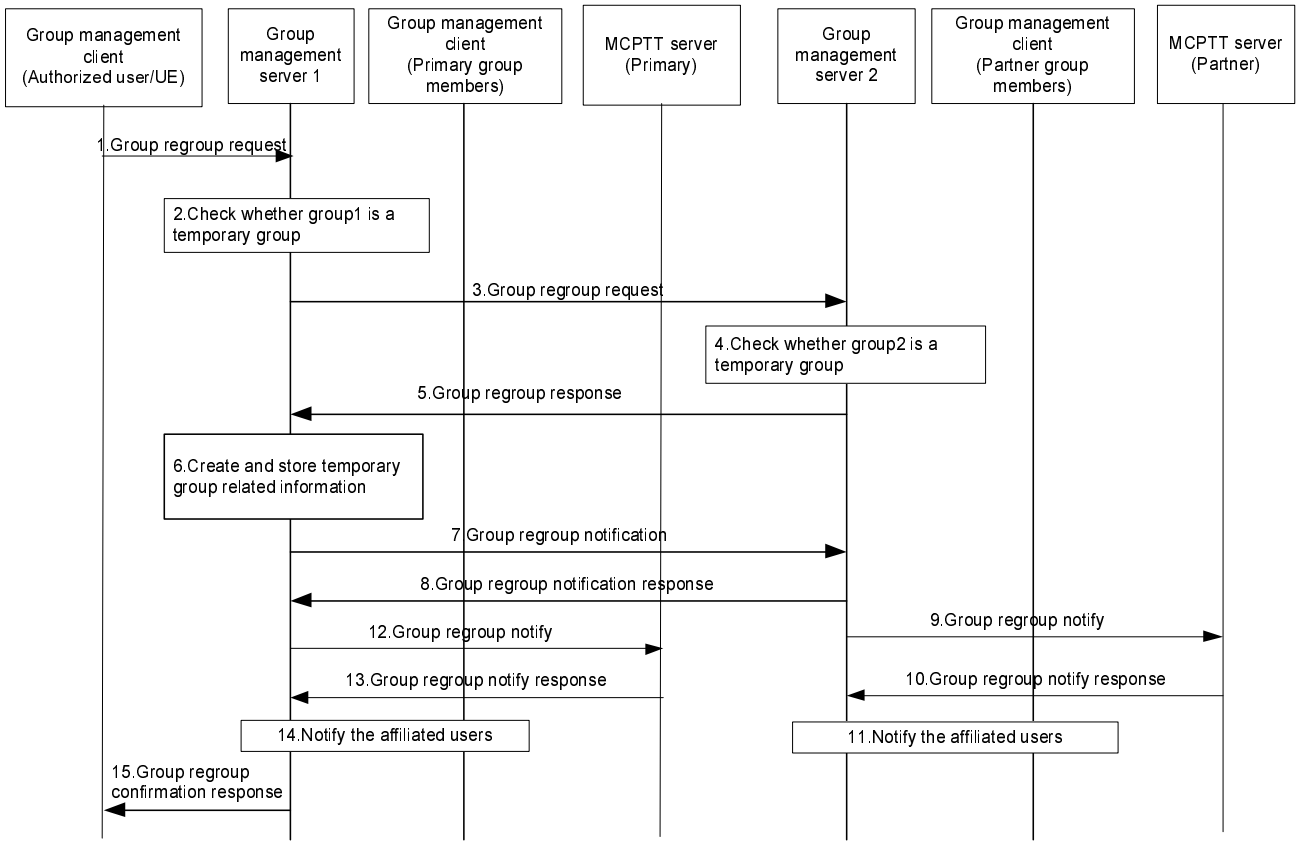

Figure 10.4.4.2-1: Temporary group formation - group regrouping involving multiple MCPTT systems

1. The group management client of the authorized MCPTT user (e.g. dispatcher) requests group regroup operation to the group management server 1 (which is the group management server of the dispatcher/authorized MCPTT user). The identities of the groups being combined shall be included in this message. The group management client may indicate the security level required for the temporary group. The group management client may indicate the priority level required for the temporary group.

2. The group management server 1 checks whether group1 is a temporary group. If group1 is a temporary group, then the group regrouping will be rejected, otherwise the group regrouping can proceed.

3. The group management server 1 forwards the group regroup request to the target group management server 2 with the information of the group management server 2 MCPTT groups.

4. The group management server 2 checks whether group2 is a temporary group. If group2 is a temporary group, then the group regrouping will be rejected, otherwise the group regrouping can proceed.

5. The group management server 2 provides a group regroup response. Due to security aspects concerning sharing information among different MCPTT systems, the group management server 2 does not share the users' information of the groups under its management to the group management server 1.

NOTE: If there is a trust relationship between the primary MCPTT service provider and the partner service provider, the partner MCPTT system can share their users' information to the primary MCPTT system at this step. If there is a change in partner MCPTT system''s constituent group membership, the synchronization procedure with the primary MCPTT system for temporary group is out of scope of this specification

6. The group management server 1 creates and stores the information of the temporary group, including the temporary group identity, off-network information, and the identities of the groups being combined, the priority level of the temporary group, and the security level of the temporary group. If the authorized MCPTT user does not specify the security level and the priority level, the group management server shall set the lower security level and the higher priority of the constituent groups.

7. The group management server 1 notifies the group management server 2 about its group regroup operation.

8. The group management server 2 acknowledges the group management server 1 and the group management server 2 also stores the information about the temporary group including the temporary group identity, the identities of the groups being combined, the priority level of the temporary group and the security level of the temporary group.

9. The group management server 2 notifies the partner MCPTT server regarding the temporary group creation with the information of the constituent groups i.e. temporary group id, group1 id and group2 id.

10. Partner MCPTT server acknowledges the notification from the group management server 2.

11. The group management server 2 notifies the affiliated MCPTT group members of the constituent MCPTT groups of the group management server 2, possibly with an indication of a lower security level.

12. The group management server 1 notifies the MCPTT server of the primary system regarding the temporary group creation with the information of the constituent groups, i.e. temporary group id, group1 id and group2 id. If there are active calls to be merged then the group management server 1 includes an indication to merge active calls.

13. Primary MCPTT server acknowledges the notification from the group management server 1.

14. The group management server 1 notifies the affiliated MCPTT group members of the constituent MCPTT groups of the group management server 1, possibly with an indication of lower security level.

15. The group management server 1 provides a group regroup confirmation response to the group management client of the authorized MCPTT user (e.g. dispatcher).

10.4.4.3 Temporary group tear down involving multiple group host servers

Figure 10.4.4.3-1 below illustrates the tearing down procedure of temporary group created through the group regroup. The procedure can be used when, e.g., the specific task for which the temporary group was created has been completed or a busier period occurs. For simplicity, only the teardown case for a temporary group with two MCPTT groups is represented. The procedure is applicable for more than two groups combined in this temporary group.

Pre-conditions:

1. The security aspects of sharing the user information between primary and partner MCPTT systems shall be governed as per the service provider agreement between them. In this case, it considers the partner MCPTT system does not share their users' information to the primary MCPTT system.

2. The primary MCPTT system consists of the group management server 1 and MCPTT server (primary). The partner MCPTT system consists of the group management server 2 and MCPTT server (partner).

3. The group management client of the authorized MCPTT user belongs to the primary MCPTT system.

4. The temporary group to be torn down is comprised of multiple MCPTT groups, and is created through the group regrouping procedure as described in subclause 10.4.4.2.

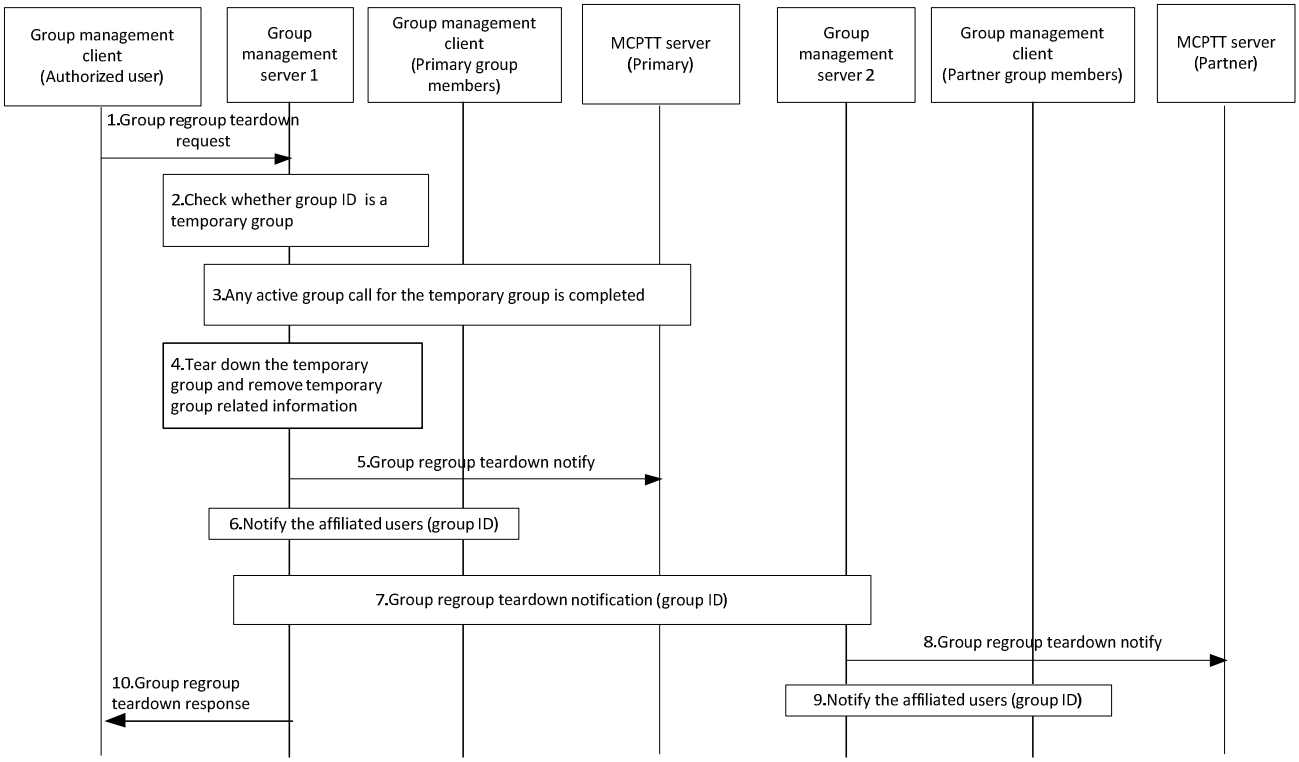

Figure 10.4.4.3-1: Temporary group tear down

1. The group management client of the authorized MCPTT user requests group regroup teardown operation to the group management server 1 (which is the group management server where the temporary group is created and stored). The identity of the temporary group (group ID) being torn down shall be included in this message. This message may route through some other signalling nodes.

2. The group management server 1 checks whether the group ID is a temporary group. If group ID is not a temporary group, then the group regroup teardown request will be rejected, otherwise the group regroup teardown can proceed.

3. Any active group call for the temporary group is completed.

4. The group management server 1 tears down the temporary group, i.e., remove the temporary group related information.

5. The group management server 1 notifies the primary MCPTT application server regarding the temporary group teardown.

6. The group management server 1 notifies the affiliated MCPTT group members regarding the temporary group teardown.

7. The group management server 1 notifies the group management server 2 – group management server in another MCPTT system regarding the temporary group teardown.

8-9. The group management server 2 notifies the partner MCPTT server and the affiliated MCPTT group members regarding the temporary group teardown.

NOTE: Step 7, 8 and 9 are only performed when the teardown of the temporary group involves constituent groups from different MCPTT systems.

10. The group management server 1 provides a group regroup teardown confirmation response to the group management client of the authorized MCPTT user.

10.5 Pre-established session

10.5.1 General

The MCPTT server may use one or more pre-established sessions for the following procedures for on-network:

- Group calls (as specified in subclause 10.6.2.3 and subclause 10.6.2.4);
- Private calls (as specified in subclause 10.7.2.2 and subclause 10.7.2.3);
- MCPTT emergency group calls (as specified in subclause 10.6.2.6.1);
- MCPTT imminent peril group calls (as specified in subclause 10.6.2.6.2);
- MCPTT emergency private calls (as specified in subclause 10.7.2.4); and
- MCPTT emergency alerts (as specified in subclause 10.6.2.6.3).

The MCPTT client establishes one or more pre-established sessions to an MCPTT server after SIP registration, and prior to initiating any of the above procedures to other MCPTT users. When establishing a pre-established session, the MCPTT client negotiates the media parameters, including establishing IP addresses and ports using interactive connectivity establishment (ICE) as specified in IETF RFC 5245 [15], which later can be used in MCPTT calls. This avoids the need to negotiate media parameters (including evaluating ICE candidates) and reserving bearer resources during the MCPTT call establishment that results in delayed MCPTT call establishment.

For outgoing MCPTT call setup for a private call or a pre-arranged group call using a pre-established session, an MCPTT UE uses SIP procedures to establish the call.

For incoming MCPTT call setup for a pre-arranged group call using a pre-established session, an MCPTT UE is notified of the start of the MCPTT call using floor control messages.

For incoming MCPTT call setup for a private call using a pre-established session, an MCPTT UE is notified of the start of the MCPTT call control using SIP procedures in manual commencement mode and using floor control procedures in automatic commencement mode.

An MCPTT UE can join an MCPTT chat group using a pre-established session by sending a group join request using SIP procedures.

NOTE: A chat group call is started and notified using floor control messages regardless of whether pre-established session is used.

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

The pre-established session may be modified by the MCPTT client and the MCPTT server using the SIP procedures for session modification.

The pre-established session may be released by the MCPTT client and the MCPTT server using the SIP procedures for terminating a SIP session.

10.5.2 Information flows for pre-established session

10.5.2.1 Pre-established session establishment

Table 10.5.2.1-1 describes the information flow create pre-established session request from the MCPTT client to the MCPTT server.

Table 10.5.2.1-1: Create pre-established session request

Information element	Status	Description
MCPTT ID of requester (originator)	M	This element identifies the MCPTT user that wishes to create a pre-established session.
SDP offer	M	SDP with media information offered by client (e.g. ports, codec, protocol id)

Table 10.5.2.1-2 describes the information flow create pre-established session response from the MCPTT server to the MCPTT client.

Table 10.5.2.1-2: Create pre-established session response

Information element	Status	Description
SDP Answer	M	SDP with media information offered by server (e.g. ports, codec, protocol id)
Session ID	M	This element identifies the specific session ID used for pre-established sessions.

10.5.2.2 Pre-established session modification

Table 10.5.2.2-1 describes the information flow modify pre-established session request from the MCPTT client to the MCPTT server.

Table 10.5.2.2-1: Modify pre-established session request

Information element	Status	Description
MCPTT ID of requester (originator)	M	This element identifies the MCPTT user that wishes to create a pre-established session.
Session ID	M	This element identifies the specific session ID used for pre-established sessions.
SDP offer	M	SDP with media information offered by client (e.g. ports, codec, protocol id).

Table 10.5.2.2-2 describes the information flow modify pre-established session response from the MCPTT server to the MCPTT client.

Table 10.5.2.2-2: Modify pre-established session response

Information element	Status	Description
SDP Answer	M	SDP with media information offered by server (e.g. ports, codec, protocol id).
Session ID	M	This element identifies the specific session ID used for pre-established sessions.

10.5.2.3 Pre-established session release - client initiated

Table 10.5.2.3-1 describes the information flow release pre-established session request from the MCPTT client to the MCPTT server.

Table 10.5.2.3-1: Release pre-established session request - client initiated

Information element	Status	Description
MCPTT ID of requester (originator)	M	This element identifies the MCPTT user that wishes to release a pre-established session.
Session ID	M	This element identifies the specific session ID used for pre-established sessions.
Release reason	M	This element indicates that reason for the session release.

Table 10.5.2.3-2 describes the information flow release pre-established session response from the MCPTT server to the MCPTT client.

Table 10.5.2.3-2: Release pre-established session response - client initiated

Information element	Status	Description
Session ID	M	This element identifies the specific session ID used for pre-established sessions.

10.5.2.4 Pre-established session release - server initiated

Table 10.5.2.4-1 describes the information flow release pre-established session request from the MCPTT server to the MCPTT client.

Table 10.5.2.4-1: Release pre-established session release request - server initiated

Information element	Status	Description
MCPTT ID of target	M	This element identifies the MCPTT user that is the target of the for pre-established session release.
Release reason	M	This element indicates that reason for the session release.

Table 10.5.2.4-2 describes the information flow release pre-established session response from the MCPTT client to the MCPTT server.

Table 10.5.2.4-2: Release pre-established session response - client initiated

Information element	Status	Description
Session ID	M	This element identifies the specific session ID used for pre-established sessions.

10.5.2.5 Pre-established session call connect request

Table 10.5.2.5-1 describes the information flow pre-established session call connect request from the MCPTT server to the MCPTT client.

Table 10.5.2.5-1: Pre-established session call connect request

Information element	Status	Description
MCPTT group ID	M	Identity of the MCPTT group
MCPTT ID	O	MCPTT ID of the inviting MCPTT user

10.5.2.6 Pre-established session call disconnect request

Table 10.5.2.1.6-1 describes the information flow pre-established session call disconnect request from the MCPTT server to the MCPTT client.

Table 10.5.2.6-1: Pre-established session call disconnect request

Information element	Status	Description
MCPTT group ID	M	Identity of the MCPTT group

10.5.3 Procedures

10.5.3.1 General

The pre-established session can be established after the initial SIP registration and MCPTT service logon. Figure 10.5.3.1-1 presents the high level description of the pre-established session procedure.

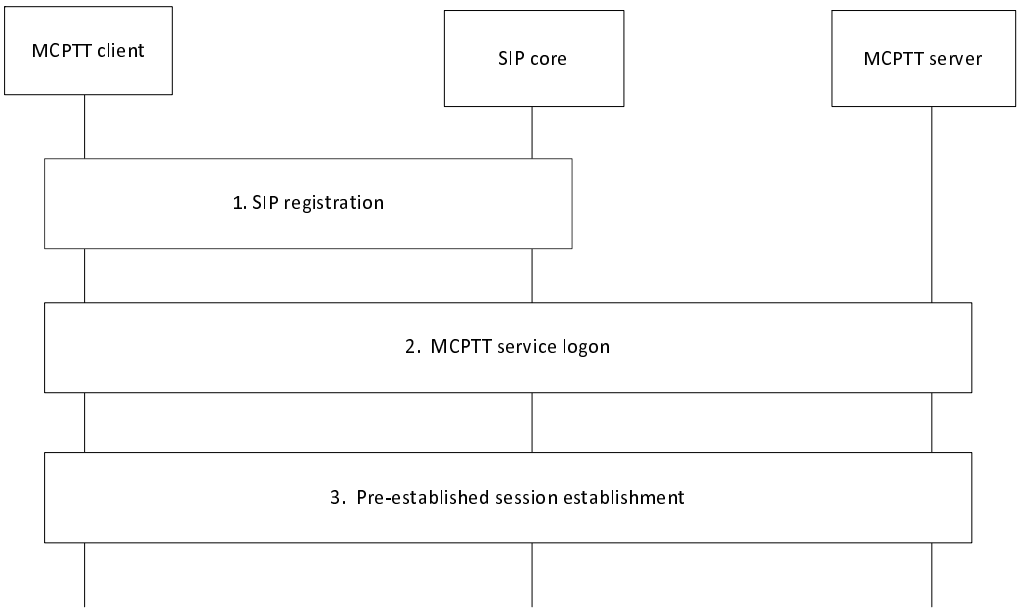

Figure 10.5.3.1-1: Pre-established session

1. The MCPTT UE in which the MCPTT client resides registers to the SIP core.
2. The user of the MCPTT client within an MCPTT UE performs a logon for the MCPTT service.
3. The pre-established session is a session establishment procedure between the MCPTT client and the MCPTT server to exchange necessary media parameters needed for the definition of the media bearers. After the pre-established session is established, the media bearer carrying the floor control messages is always active. Additionally, the MCPTT client is able to activate the media bearer carrying the voice whenever needed:
   - immediately after the pre-established session procedure; or
   - using SIP signalling when an MCPTT call is initiated.

10.5.3.2 Pre-established session establishment

The pre-established session is a session between the MCPTT client and the MCPTT server in the MCPTT system, and which may utilise other functional entities (e.g. a media distribution function, as defined in subclause 7.4.2.3.5, for means of obtaining media parameters and gathering ICE candidates). Figure 10.5.3.2-1 represents the pre-established session establishment flow.

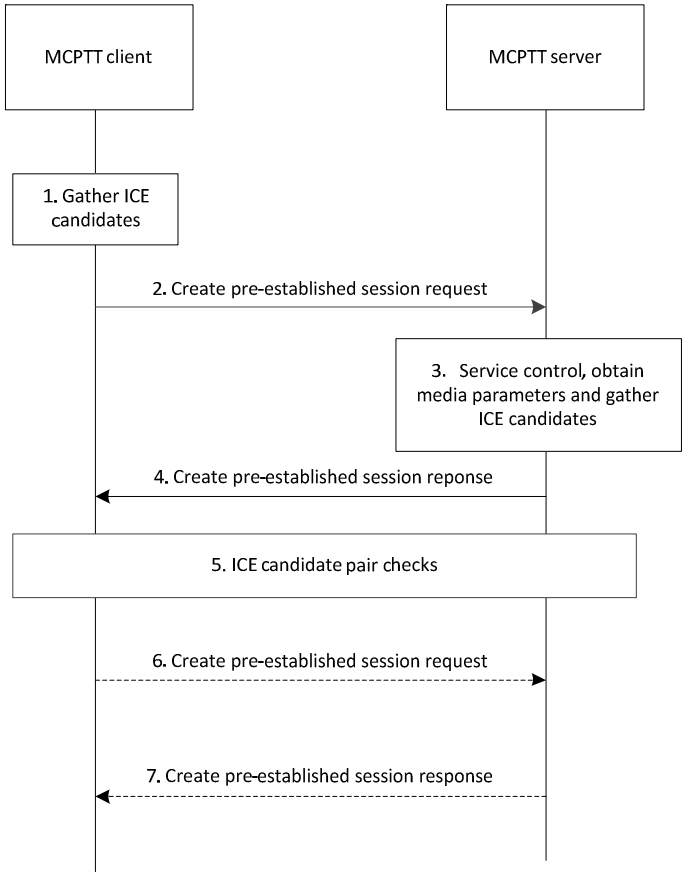

Figure 10.5.3.2-1: Pre-established session establishment

1. The MCPTT client within the MCPTT UE gathers ICE candidates.
2. The MCPTT client within the MCPTT UE sends a request to the MCPTT server to create a pre-established session.
3. MCPTT server performs necessary service control, obtains media parameters (e.g. by means of interacting with a media distribution function of the MCPTT server) and gathers ICE candidates.
4. MCPTT server sends an OK response to the MCPTT client within the MCPTT UE.
5. ICE candidate pair checks take place e.g. between the MCPTT client within the MCPTT UE and a media distribution function of the MCPTT server.
6. If necessary the MCPTT client within the MCPTT UE sends another request to the MCPTT server to update the ICE candidate pair for the pre-established session.
7. The MCPTT server sends an OK response accepting the ICE candidate pair update.

The media sessions are consisting of at least an active media session carrying the floor control messages with bearer of QCI 'Mission Critical delay sensitive signalling' and an inactive media session for the voice media (which is carried when active by a GBR of QCI 'Mission Critical user plane Push To Talk voice').

NOTE: The mission critical specific QCIs are defined in 3GPP TS 23.203 [4].

10.5.3.3 Pre-established session modification

Figure 10.5.3.3-1 represents the pre-established session establishment flow.

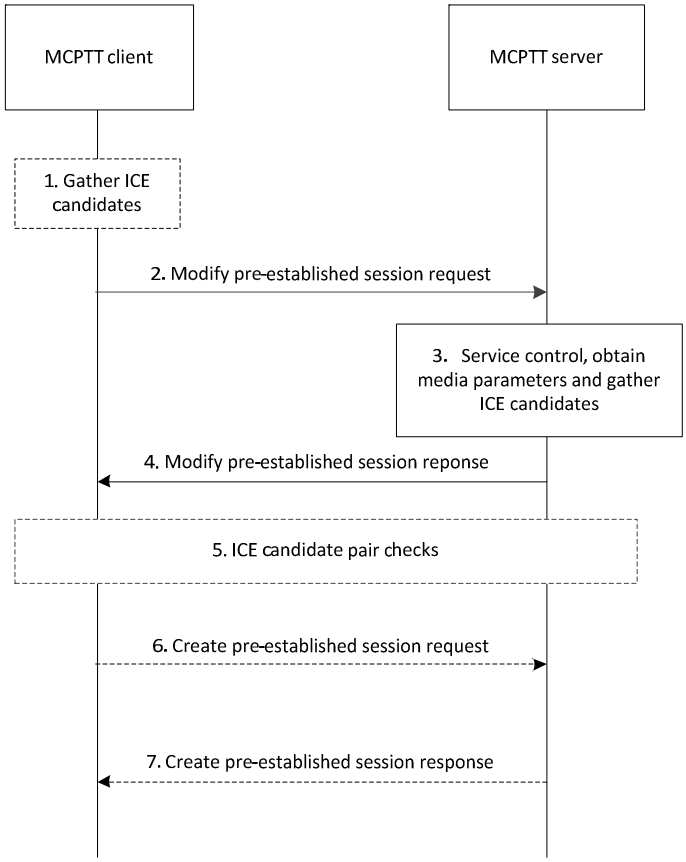

Figure 10.5.3.3-1: Pre-established session modification

1. The MCPTT client within the MCPTT UE gathers ICE candidates, if necessary (e.g. depending on the information that needs to be updated).

2. The MCPTT client within the MCPTT UE sends a request to the MCPTT server to modify a pre-established session.

3. MCPTT server performs necessary service control, obtains any necessary media parameters (e.g. by means of interacting with a media distribution function of the MCPTT server) and gathers necessary ICE candidates.

4. MCPTT server sends an OK response to the MCPTT client within the MCPTT UE.

5. If necessary, ICE candidate pair checks take place e.g. between the MCPTT client within the MCPTT UE and a media distribution function of the MCPTT server.

6. If necessary the MCPTT client within the MCPTT UE sends another request to the MCPTT server to update the ICE candidate pair for the pre-established session.

7. The MCPTT server sends an OK response accepting the ICE candidate pair update.

NOTE 1: The represented procedure corresponds to a session modification initiated by the MCPTT client. It can also be initiated by the MCPTT server.

NOTE 2: The procedure can also be used to switch a media session from the inactive to the active state and the reverse. The modification of the session triggers a corresponding modification of the characteristics (activity, bandwidth,..) of the corresponding GBR bearers.

10.5.3.4 Pre-established session release

Figure 10.5.3.4-1 represents the MCPTT client within the MCPTT UE initiated pre-established session release flow and figure 10.5.3.4-2 represents the MCPTT server initiated pre-established session release flow.

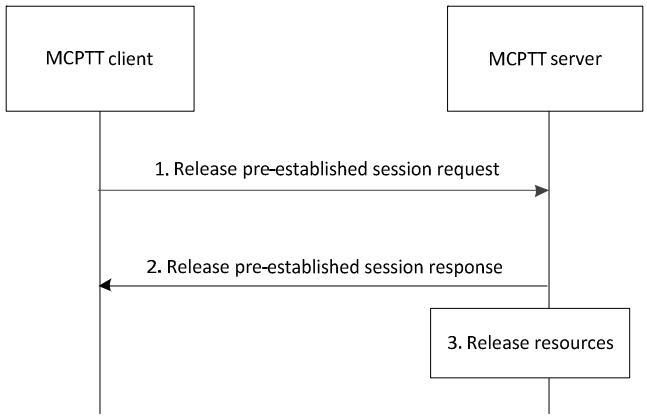

Figure 10.5.3.4-1: MCPTT client within the MCPTT UE initiated pre-established session release

1. The MCPTT client within the MCPTT UE sends a request to the MCPTT server to release a pre-established session.
2. The MCPTT server sends an OK response to the MCPTT client within the MCPTT UE.
3. The MCPTT server releases all resources for the pre-established session.

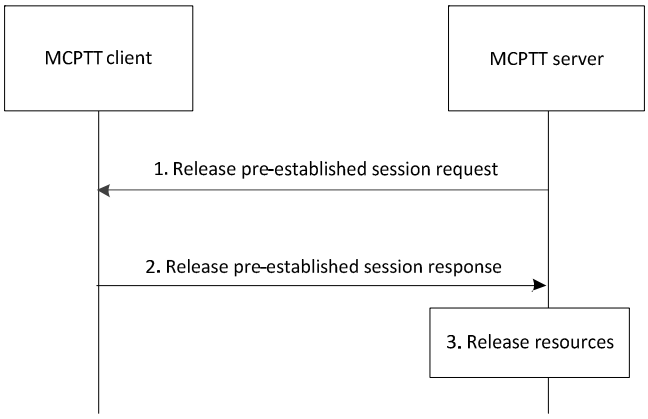

Figure 10.5.3.4-2: MCPTT Server initiated pre-established session release

1. The MCPTT server sends a request to the MCPTT client within the MCPTT UE to release a pre-established session.
2. The MCPTT client within the MCPTT UE sends an OK response to the MCPTT server.
3. The MCPTT server releases all resources for the pre-established session.

10.5.3.5 Call connect and disconnect procedures using pre-established session

10.5.3.5.1 Call connect and disconnect over unicast

Call connect and disconnect information flows are sent over non-SIP media plane signalling using MCPTT-4 for including or releasing an MCPTT client in the call using a pre-established session.

Figure 10.5.3.5.1-1 shows the high level procedure where a call connect information flow is sent by the MCPTT server to inform MCPTT client(s) using a pre-established session that the MCPTT client(s) has/have been connected to an MCPTT private call or group call.

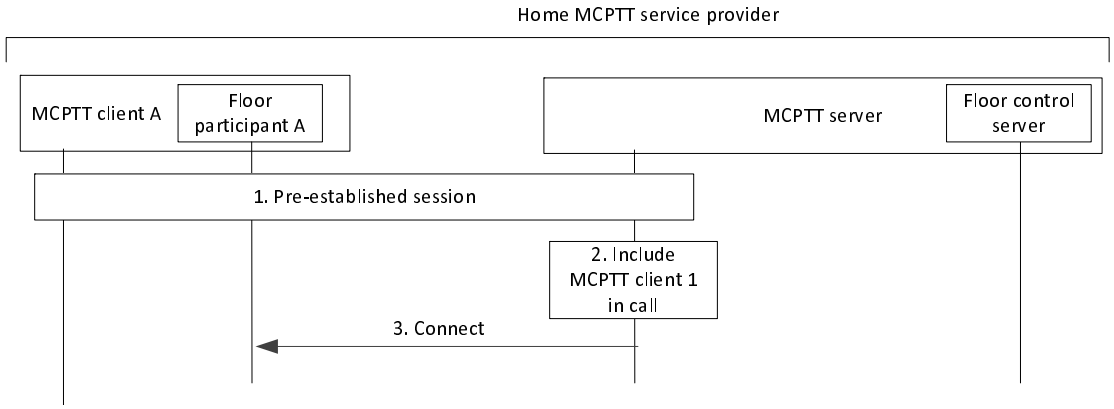

Figure 10.5.3.5.1-1: Connect procedure

1. Pre-established session exists between MCPTT client A and MCPTT server.
2. MCPTT server has determined to include MCPTT client A in the call e.g., upon receiving the request from another MCPTT client to include MCPTT client A in the call.
3. Connect information flow is sent by the MCPTT server to inform MCPTT client A using a pre-established session that it has been connected to MCPTT private or group call. The floor control is established between floor participant A and floor control server.

Figure 10.5.3.5.1-2 shows the high level procedure where a disconnect information flow is sent by the MCPTT server to the MCPTT client A to indicate that the MCPTT private call or group call using a pre-established session has been released.

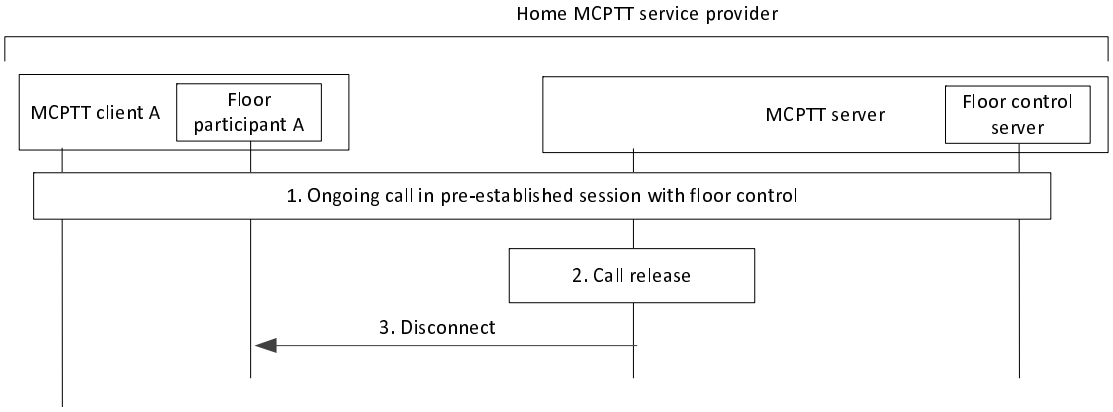

Figure 10.5.3.5.1-2: Disconnect procedure

1. Floor control is ongoing within a private or group call established using pre-established session.

2. MCPTT server has determined to release MCPTT client A from the call e.g., due to call release.

3. Disconnect message is sent by the MCPTT server to indicate to MCPTT client A that the MCPTT private call or group call using a pre-established session has been released. Pre-established session between MCPTT client A and MCPTT server remains for further use.

10.6 Group call

10.6.1 General

Group calls are enabled in both on-network and off-network.

10.6.2 On-network group call

10.6.2.1 General

This subclause contains procedures for group call across a single and multiple MCPTT servers, and associated functions such as emergency call, broadcast call and others.

Two variations of group call model are described in subclause 10.6.2.3, the pre-arranged group call and the chat group call. Each of the subsequent group call types in subclause 10.6.2.4 onwards are applicable to either call model.

10.6.2.2 Information flows for group call in on-network

10.6.2.2.1 MCPTT emergency group call request

Table 10.6.2.2.1-1 describes the information flow emergency group call request from the MCPTT client to the MCPTT server.

Table 10.6.2.2.1-1 MCPTT emergency group call request information elements

Information Element	Status	Description
MCPTT ID	M	The identity of the calling party
Group ID	M	The group identity on which the call is to be conducted
Emergency indicator	M	Indicates that the group call request is an MCPTT emergency call
Alert indicator	M	Indicates whether an emergency alert is to be sent

10.6.2.2.2 MCPTT emergency group call cancel request

Table 10.6.2.2.2-1 describes the information flow emergency group call cancel request from the MCPTT client to the MCPTT server.

Table 10.6.2.2.2-1 MCPTT emergency group call cancel request information elements

Information Element	Status	Description
MCPTT ID	M	The identity of the cancelling party
Group ID	M	The group identity on which the MCPTT emergency is in progress
Alert indicator	O	Indicates whether the emergency alert is to be cancelled

10.6.2.2.3 MCPTT emergency alert request

Table 10.6.2.2.3-1 describes the information flow MCPTT emergency alert request from the MCPTT client to the MCPTT server.

Table 10.6.2.2.3-1 MCPTT emergency alert request information elements

Information Element	Status	Description
MCPTT ID	M	The identity of the alerting party
Group ID	M	The group identity with which the alert is associated

10.6.2.2.4 MCPTT emergency state cancel request

Table 10.6.2.2.4-1 describes the information flow MCPTT emergency state cancel request from the MCPTT client to the MCPTT server.

Table 10.6.2.2.4-1 MCPTT emergency state cancel request information elements

Information Element	Status	Description
MCPTT ID	M	The identity of the cancelling party
MCPTT group ID	M	The group identity with which the alert is associated
Client emergency state cancel inform (NOTE)	O	Requests cancellation of the emergency state associated with this MCPTT client
Group emergency condition cancel request (NOTE)	O	Requests cancellation of the emergency condition of the group
NOTE: At least one of these information elements shall be present		

10.6.2.2.5 MCPTT imminent peril group call request

Table 10.6.2.2.5-1 describes the information flow MCPTT imminent peril group call request from the MCPTT client to the MCPTT server.

Table 10.6.2.2.5-1 MCPTT imminent peril group call request information elements

Information Element	Status	Description
MCPTT ID	M	The identity of the calling party
Group ID	M	The group identity on which the call is to be conducted
Imminent peril indicator	M	Indicates that the group call request is an imminent peril call

10.6.2.2.6 MCPTT imminent peril group call cancel request

Table 10.6.2.2.6-1 describes the information flow MCPTT imminent peril group call cancel request from the MCPTT client to the MCPTT server.

Table 10.6.2.2.6-1 MCPTT imminent peril group call cancel request information elements

Information Element	Status	Description
MCPTT ID	M	The identity of the cancelling party
Group ID	M	The group identity on which the imminent peril is to be cancelled

10.6.2.3 Group call within one MCPTT system

10.6.2.3.1 Group call models

10.6.2.3.1.1 Pre-arranged group call

10.8.2.3.1.1.1 General

A pre-arranged group call is initiated by one of the group members. The initiation of a pre-arranged group call results in all other affiliated group members being invited.

10.6.2.3.1.1.2 Pre-arranged group call setup

The procedure focuses on the case where an MCPTT client is initiating an MCPTT group call with unicast signalling for communicating with the affiliated MCPTT members of that group.

Procedures in figure 10.6.2.3.1.1.2-1 are the signalling control plane procedures for the MCPTT client initiating establishment of an MCPTT group call with a pre-arranged group i.e., MCPTT users on client 1, client 2 and client 3 belong to the same group which is defined in the MCPTT group management server.

Pre-conditions:

1. A pre-arranged group is an MCPTT group that is pre-defined with MCPTT group ID and member list in the group management server. All members of the group belong to the same MCPTT system.
2. It is assumed that MCPTT users on MCPTT client 1, MCPTT client 2 and MCPTT client 3 are already registered for receiving MCPTT service and affiliated.

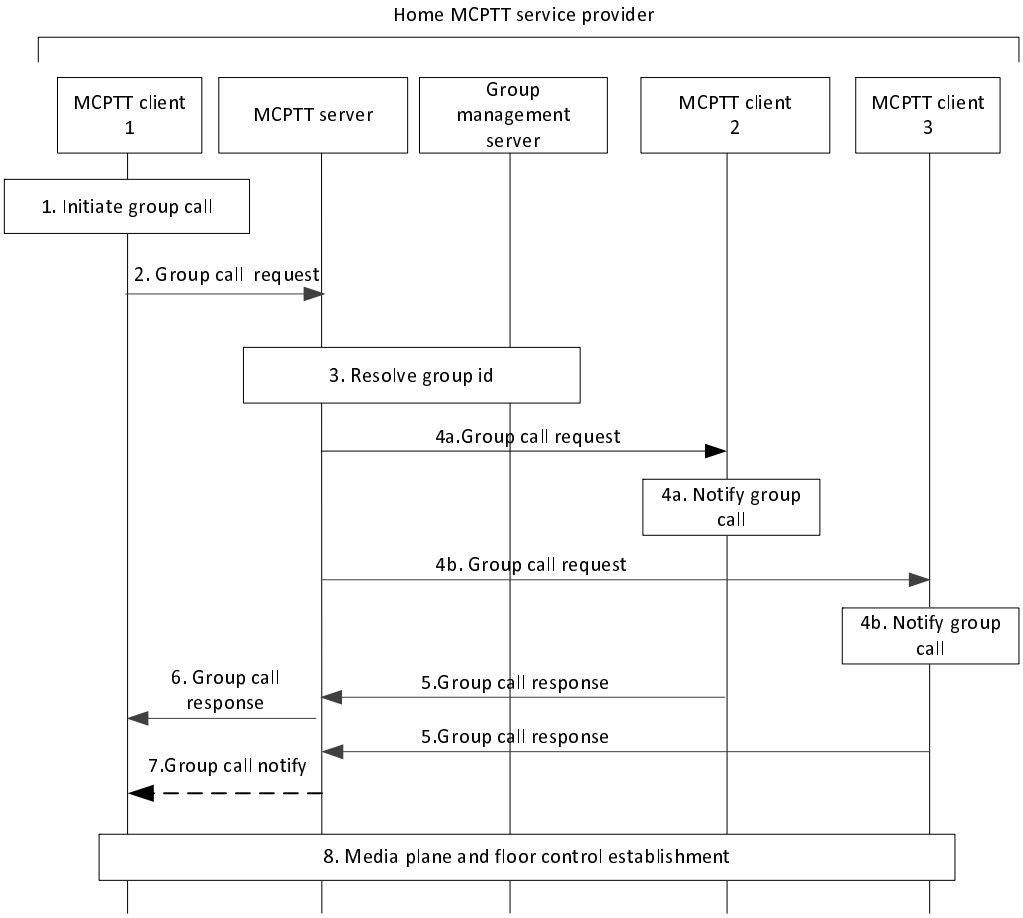

Figure 10.6.2.3.1.1.2-1: Pre-arranged group call setup

1. User at MCPTT client 1 would like to initiate an MCPTT group call with a selected group (identified by MCPTT group ID).

NOTE 1: MCPTT client 1 need not be aware of the affiliation status of other MCPTT clients to the group while initiating the group call.

2. MCPTT client 1 sends a group call request towards the MCPTT server via the SIP core, which hosts the group selected by the user and identified by MCPTT group ID. The group call request also contains the MCPTT group ID and an SDP offer containing the MCPTT client media parameters. If there is a request to transmit, then the group call request contains an indication of an implicit floor request.

3. MCPTT server checks whether the user of MCPTT client 1 is authorized to initiate a group call for the selected group. If authorized and the group call is ongoing for that MCPTT group ID, the MCPTT server adds the requesting MCPTT client 1 to the existing MCPTT group call and notifies the MCPTT client 1 that the MCPTT group call is already in progress. Otherwise, MCPTT server resolves the MCPTT group ID to determine the members of that group and their affiliation status, based on the information from the group management server.

NOTE 2: MCPTT server can have already retrieved the user/group policy from the group management server and locally cached. If the user/group policy is not locally cached on the MCPTT server then MCPTT server requests the user/group policy from the group management server.

4. MCPTT server includes information that it communicates using MCPTT service, offers the same media parameters or a subset of the media parameters contained in the initial received request and sends the corresponding group call request via the SIP core towards the MCPTT clients of each of those affiliated group members. MCPTT users are notified about the incoming group call. The MCPTT server indicates whether acknowledgement is required for the call.

5. The receiving MCPTT clients accept the group call request, and a group call response is sent to the group host MCPTT server. This response may contain an acknowledgement. The conditions for sending acknowledgement may be based on configuration.

6. MCPTT server sends the group call response including the selected media parameters to the MCPTT client 1 through the signalling path to inform about successful call establishment.

NOTE 3: Step 6 can occur at any time following step 4b, and prior to step 7 depending on the conditions to proceed with the call.

7. If the initiating MCPTT user requires the acknowledgement from affiliated MCPTT group members, and the required MCPTT group members do not acknowledge the call setup within a configured time (the "acknowledged call setup timeout"), then the MCPTT server may proceed with or abandon the call and then notify the initiating MCPTT user that the acknowledgements did not include all required members according to group policy. This notification may be sent to the initiating MCPTT user by the MCPTT server more than once during the call when MCPTT users join or leave the MCPTT group call.

8. MCPTT client 1, client 2 and client 3 have successfully established media plane for communication. MCPTT floor participant 1, floor participant 2 and floor participant 3 exchange floor control information e.g., MCPTT client 1 receives the floor granted information over the established media plane assuming implicit floor control request from MCPTT client 1 while at the same time floor participants at other MCPTT client's receive floor taken information. MCPTT client 1 indicates to the MCPTT user that the floor is available to send media, while the other MCPTT clients in the group call will be receiving that media.

10.6.2.3.1.1.3 Release pre-arranged group call

The procedures focuses on the case where an MCPTT server initiates the termination of an ongoing MCPTT group call for all the participants of that group call, since at least one of the termination conditions are met e.g., due to hang time expiry, last participant leaving, second last participant leaving, initiator leaving, or minimum number of affiliated MCPTT group members are not present.

NOTE: The procedure for MCPTT user leaving the group call is a different scenario and is not considered in this solution.

Procedures in figure 10.6.2.3.1.1.3-1 are the signalling control plane procedures for the MCPTT server initiating termination of an ongoing MCPTT group call.

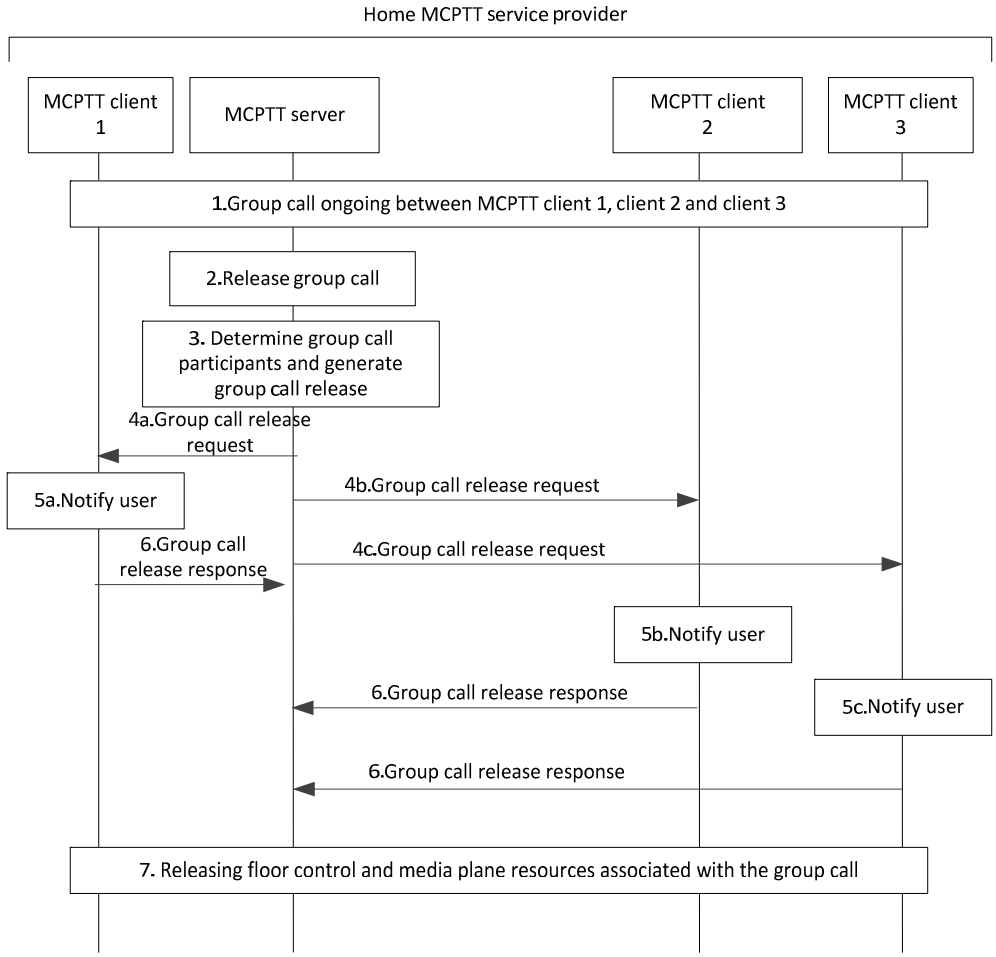

Figure 10.6.2.3.1.1.3-1: Release pre-arranged group call

1. It is assumed that MCPTT users on MCPTT client 1, client 2 and client 3 are already part of the ongoing group call (e.g., as a result of pre-arranged group call setup).

2. MCPTT server would like to release the MCPTT group call which is ongoing e.g., due to hang time expiry, due to hang time expiry, last participant leaving, second last participant leaving, initiator leaving, or minimum number of affiliated MCPTT group members are not present.

3. MCPTT server identifies the participants of the ongoing group call and generates group call release request to release ongoing session.

4. MCPTT server sends a group call release request via SIP core towards each participant of the ongoing group call.

5. MCPTT users are notified about the release of the group call.

6. MCPTT client(s) receiving group call release request, acknowledge towards the MCPTT server by sending a group call release response.

7. MCPTT client 1, client 2 and client 3 have successfully released the floor control and media plane resources associated with the group call that is terminated.

10.6.2.3.1.1.4 Late entry pre-arranged group call

Procedures in figure 10.6.2.3.1.1.4-1 are the signalling control plane procedures for the MCPTT server requesting a newly affiliated member or a member coming back from out of coverage to join an ongoing MCPTT group call.

Pre-condition:

1. MCPTT group is previously defined on the group management server with MCPTT users affiliated to that group. All members of the group belong to the same MCPTT system.

2. It is assumed that MCPTT users on MCPTT client 2 to MCPTT client n are on an ongoing call.

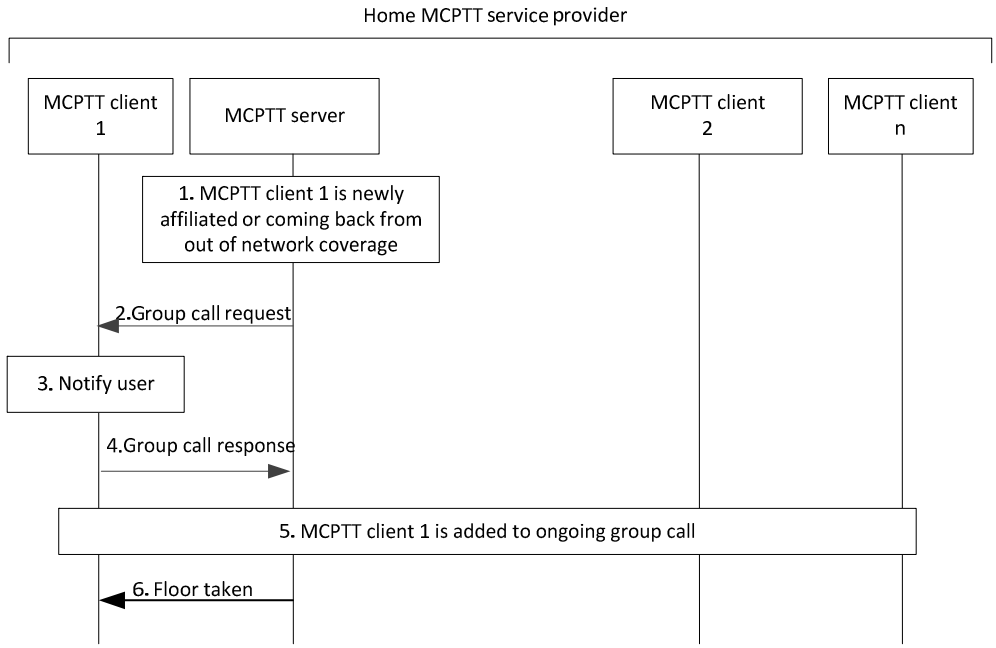

Figure 10.6.2.3.1.1.4-1: Late entry pre-arranged group call

1. MCPTT server determines that MCPTT client 1 which is newly affiliated or coming back from out of coverage has to be invited to join an ongoing group call (late entry).

2. MCPTT server generates group call request including the information such as MCPTT service identifier (possible for the SIP core to route the request to the MCPTT server), MCPTT group ID of the group invited to join, offer one or more media types and sends towards the MCPTT client 1 via SIP core.

3. MCPTT user at MCPTT client 1 is notified about the incoming group call.

4. Upon MCPTT user at MCPTT client 1 accepting the incoming group call request, MCPTT client 1 sends the group call response including the selected media types to the MCPTT server through the signalling path. If the incoming group call request is rejected by the MCPTT client 1, the MCPTT server should not resend the group call request

5. MCPTT client 1 is successfully added to the ongoing group call and MCPTT users at MCPTT client 1 to MCPTT client n may be notified about the MCPTT client 1 joining the group call.

6. The floor taken with the information of the current talker is sent to MCPTT client1.

10.6.2.3.1.1.5 Rejoining call

Procedures in figure 10.6.2.3.1.1.5-1 are the signalling control plane procedures for the MCPTT client coming back from out of coverage to rejoin an ongoing MCPTT group call.

Pre-conditions:

- It is assumed that MCPTT users on MCPTT client 2 to MCPTT client n are on an ongoing call.

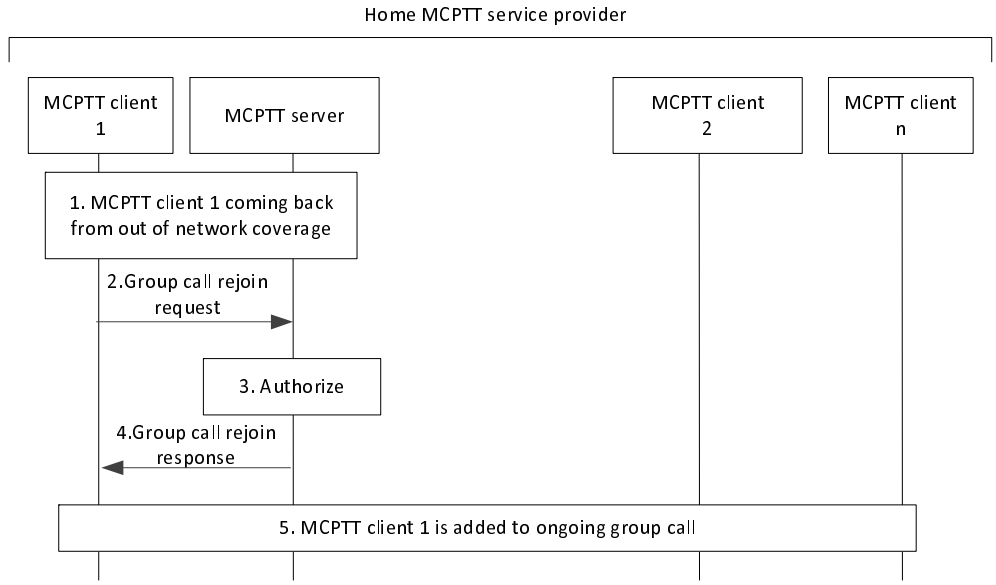

Figure 10.6.2.3.1.1.5-1: Rejoin call

1. MCPTT client 1 is coming back from out of coverage.
2. MCPTT client 1 coming back from out of coverage has necessary information for rejoining an ongoing group call, then the MCPTT client 1 initiates group call rejoin request including the ongoing group call information.
3. MCPTT client 1 is authorized for rejoining the ongoing call.
4. MCPTT client 1 is informed that the group call rejoin is successful by sending a group call rejoin response.
5. MCPTT client 1 is successfully added to the ongoing group call and MCPTT users at MCPTT client 1 to MCPTT client n may be notified about the MCPTT client 1 joining the group call.
6. The floor taken with the information of the current talker is sent to MCPTT client1.

10.6.2.3.1.2 Chat group call

10.6.2.3.1.2.1 General

In a chat group (restricted) call model, the MCPTT user individually joins a group call without being invited. The establishment of a chat group (restricted) call does not result in other group members being invited.

Figure 10.6.2.3.1.2.2-1 describes the basic procedure for the MCPTT client initiating an MCPTT group call which uses the chat group (restricted) call model. Restricted means that only users that have been configured as members of the given group are allowed to join the group communications for the given group.

Chat group join mechanism:

- Each MCPTT client sends a group join request when the MCPTT user wants to participate in the group communication for the group. (This message does not impact the MCPTT user's membership in the group; the MCPTT server will verify that the MCPTT user is an authorized member of the group.)
- The group join request may include a request to transmit. It is assumed that the group join request will be delivered from MCPTT client to MCPTT server using SIP.
- The group join request is used to indicate to the MCPTT server that the MCPTT user associated with the given MCPTT client wishes to participate (begin to receive media) from the group.
- The group join request may cause the MCPTT server to generate an implicit affiliation for the MCPTT user to the group, if the user is not already affiliated to the group.

- The group join request normally contains the information needed to negotiate media parameters between MCPTT server and MCPTT client for the group call. The group join request can take the form of a SIP invite.

Subsequent participation in a group call when the group is using the chat model:

- Once an MCPTT client successfully joins a group call which is using the chat model, the MCPTT client connects to the media plane for the call if the call is currently ongoing.

- If the MCPTT group call is not currently ongoing (i.e.: when MCPTT clients on the group call are not sending or receiving media, and the time out between floor control exchanges has expired) then the newly joined MCPTT client will only have pre-established its media parameters for the call.

- If the newly joined MCPTT user wishes to transmit media (start or re-start the call) to the affiliated users of the group using the chat model, then the MCPTT client using its associated floor control participant would follow a normal floor control procedure for requesting the floor.

- Since subsequent group call media transmissions are controlled using floor control signalling, additional SIP signalling messages may not be required for subsequent call stop and start.

- Each request to transmit from an MCPTT user could be viewed as a new instance of a group call for the given group when the floor idle timer expires and no media is present for an extended time.

- The MCPTT server may tear down the media plane between successive group calls using the chat model, or the MCPTT server may allow the media plane to remain up between successive group calls using the chat model depending on resources.

10.6.2.3.1.2.2 Chat group call setup

MCPTT client 1, client 2, and client 3 are served by the home MCPTT service provider in figure 10.6.2.3.1.2.2-1.

Pre-condition:

1. The MCPTT server may use the group join request to generate an implicit affiliation (using the affiliation procedure in subclause 10.3.3) on behalf of the client that sends the MCPTT group join request.

2. MCPTT user 2 and MCPTT user 3 have previously joined (affiliated) to the group. MCPTT client 1, client 2, and client 3 are registered and all users (MCPTT user 1, user 2, and user 3) have been authenticated and authorized to use the MCPTT service. No call is currently in progress for the group.

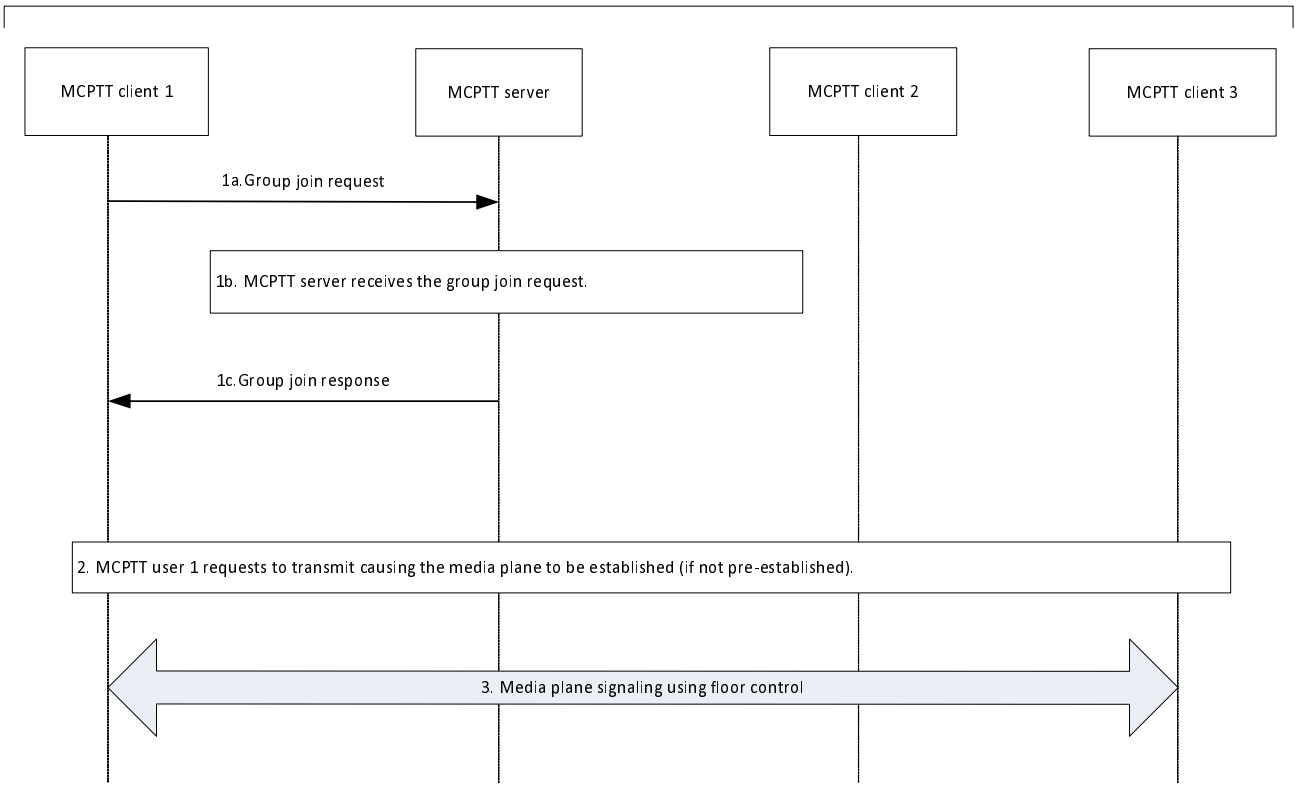

Figure 10.6.2.3.1.2.2-1: MCPTT chat group call

1. MCPTT user 1 indicates to join the group communication for the group. This may include a request to transmit.

1a. MCPTT client 1 sends a group join request with the MCPTT group ID of the desired group. It contains the MCPTT user's MCPTT ID and the MCPTT client media parameters. If there is a request to transmit, then the group joint request contains an indication of an implicit floor request.

1b. The MCPTT server receives the group join request. MCPTT server generates an implicit affiliation (if the MCPTT user is not already affiliated to the group) and verifies that MCPTT user 1 is authorized to affiliate to the group by following the affiliation procedure (subclause 10.3.3).

1c. The MCPTT server replies with a group join response indicating the acceptance of the group join request and also returns the MCPTT server selected media parameters for the group call in the group join response.

2. If MCPTT user 1 requests to transmit, the MCPTT server establishes the media plane (if not already established) for the call. The associated floor participants for MCPTT client 1, client 2, and client 3 use the floor control procedure to initiate the call. E.g., the floor participant for MCPTT client 1 receives the MCPTT floor grant. The corresponding floor participants for MCPTT client 2 and MCPTT client 3 receive the MCPTT floor taken.

3. Floor control will continue to be used by the floor participants associated with MCPTT client 1, MCPTT client 2 and MCPTT client 3 for the duration of the call. Media plane signalling using floor control will be used for subsequent calls for the group as long as one or more users are affiliated.

10.6.2.3.1.2.3 Release chat group call

The procedure describes the case where the MCPTT server releases an ongoing MCPTT group call for all the participants of that group call, since at least one of the conditions for release are met e.g. due to hang time expiry, last participant leaving, second last participant leaving, initiator leaving, or the number of affiliated MCPTT group members is below the minimum number permitted.

NOTE 1: The procedure for an MCPTT user leaving the group call is a different procedure.

Procedures in figure 10.6.2.3.1.2.3-1 are the procedures for the MCPTT server initiating the release of an ongoing MCPTT group call.

The following precondition applies:

- A group call is ongoing between MCPTT clients 1, 2 and 3

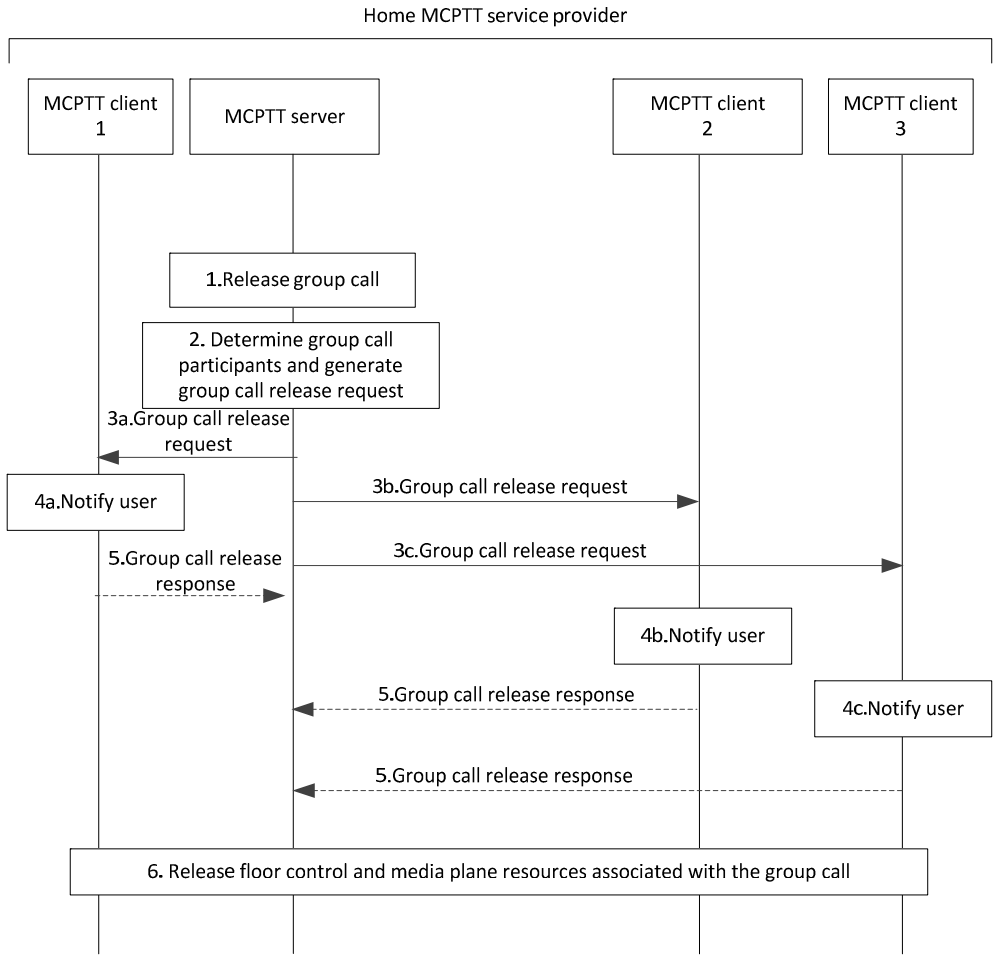

Figure 10.6.2.3.1.2.3-1: Release chat group call

1. MCPTT server would like to release the MCPTT group call which is ongoing e.g., due to hang time expiry, due to hang time expiry, last participant leaving, second last participant leaving, initiator leaving, or minimum number of affiliated MCPTT group members are not present.

2. MCPTT server identifies the participants of the ongoing group call and generates group call release request to release the ongoing session.

3. MCPTT server sends a group call release request towards each participant of the ongoing group call.

NOTE 2: The group call release request can also be sent over SIP signalling on the signalling plane.

4. MCPTT users are notified about the release of the group call.

5. Optionally the MCPTT client(s) receiving group call release request, may send a group call release response to the MCPTT server.

NOTE 3: The MCPTT client can send group call release response when the group call release request is sent using a unicast bearer.

6. MCPTT client 1, client 2 and client 3 release the floor control and media plane resources associated with the group call that is released. Successful release of the group call does not affect the status of affiliation of any of the clients.

10.6.2.3.1.2.4 Late entry chat group call

Procedures in figure 10.6.2.3.1.2.4-1 are those for the MCPTT server requesting a group member that is newly affiliated or coming back from out of coverage to join an ongoing MCPTT group call.

Pre-conditions:

1. MCPTT group is previously defined on the group management server with MCPTT users affiliated to that group. All members of the group belong to the same MCPTT system.
2. MCPTT users using MCPTT client 2 to MCPTT client n are in an ongoing call.

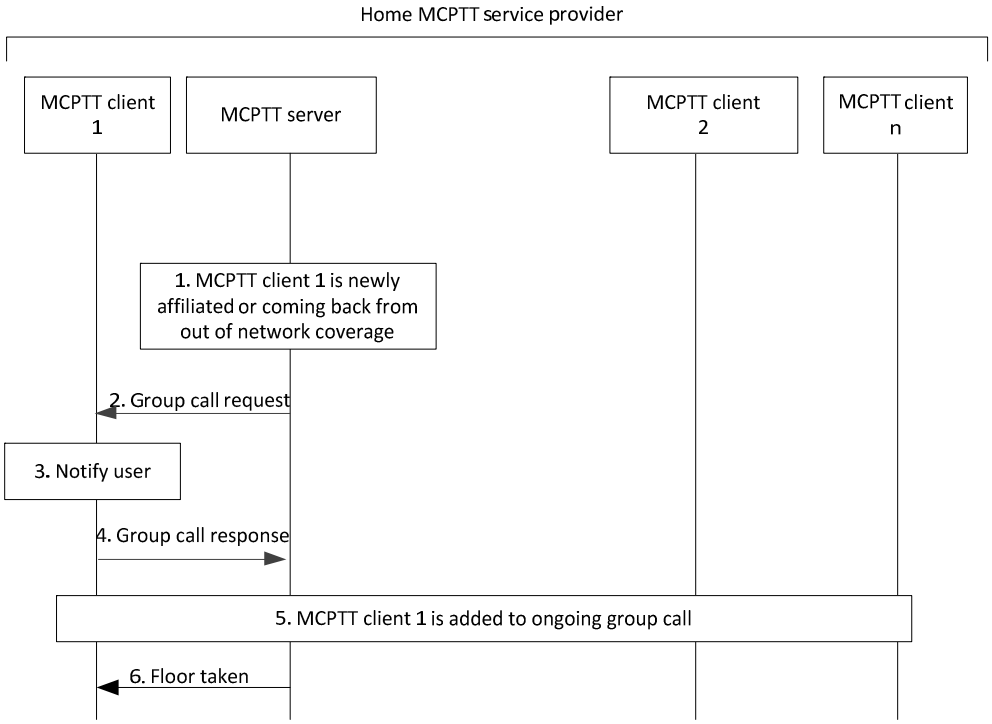

Figure 10.6.2.3.1.2.4-1: Late entry chat group call

1. MCPTT server determines that MCPTT client 1 which is newly affiliated or has returned from being out of coverage has to be requested to join an ongoing group call (late entry).
2. MCPTT server sends group call request to MCPTT client 1.
3. MCPTT user at MCPTT client 1 is notified about the incoming group call.
4. Upon MCPTT user at MCPTT client 1 accepting the incoming request, MCPTT client 1 sends a group call response to the MCPTT server. If the incoming request is rejected by MCPTT client 1, the MCPTT server should not resend the group call request.
5. MCPTT client 1 is successfully added to the ongoing group call and MCPTT users at MCPTT client 1 to MCPTT client n may be notified about the MCPTT client 1 joining the group call.
6. Floor taken with the information of the current talker is sent to MCPTT client 1.

10.6.2.3.2 Exiting group call due to de-affiliation

Procedures in figure 10.6.2.3.2-1 are the signalling control plane procedures for the MCPTT server requesting a newly de-affiliated member to leave an ongoing MCPTT group call.

Pre-conditions:

1. MCPTT group is previously defined on the group management server with MCPTT users affiliated to that group. All members of the group belong to the same MCPTT system.

2. MCPTT users on MCPTT client 1 to MCPTT client n are on an ongoing call.
3. MCPTT client 1 has been de-affiliated from the MCPTT group.

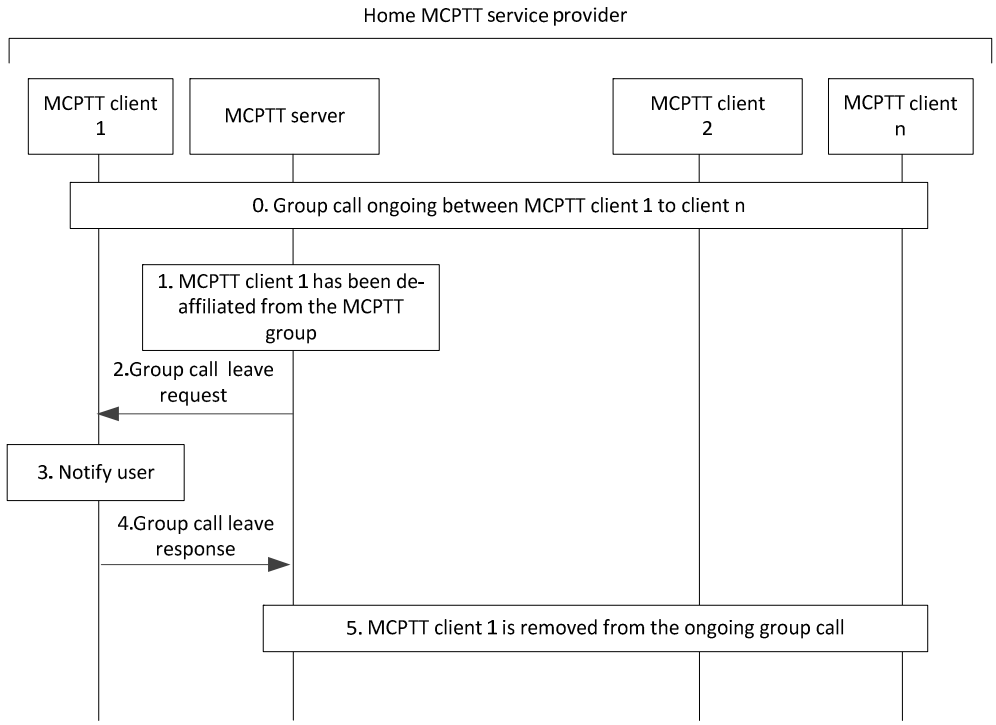

Figure 10.6.2.3.2-1: Exiting MCPTT group call due to de-affiliation

1. MCPTT client 1 which has been de-affiliated is instructed to leave the ongoing group call.
2. MCPTT server sends a group call leave request to MCPTT client 1.
3. MCPTT user at MCPTT client 1 is notified about leaving the group call.
4. MCPTT client 1 sends the group call leave response and leaves the group call.
5. MCPTT client 1 is now removed from the ongoing group call and MCPTT users at MCPTT client 2 to MCPTT client n may be notified that MCPTT client 1 has left the group call.

10.6.2.4 Group call involving groups from multiple MCPTT systems

10.6.2.4.1 Group call for temporary groups across multiple MCPTT systems

10.6.2.4.1.1 Group call setup

10.6.2.4.1.1.1 Group call setup procedure – originating side

Figure 10.6.2.4.1.1.1-1 illustrates the originating side group call involving groups from multiple MCPTT systems. It considers the scenario for group hierarchies and temporary groups formed by group regroup. The protocol followed may be SIP.

Pre-conditions:

1. The security aspects of sharing the user information between primary and partner MCPTT systems shall be governed as per the service provider agreement between them. In this case, we consider the partner MCPTT system does not share their users' information to the primary MCPTT system.

2. The MCPTT user belongs to an MCPTT group hosted by the primary MCPTT system.

3. A temporary group is formed by authorized MCPTT user/dispatcher by the group regroup procedure (subclause 10.4.4.2) and identified via a temporary group ID.

4. The MCPTT group members of the constituent MCPTT groups belonging to the temporary group are affiliated to participate in a group call for the temporary group.

5. The authorized MCPTT user/dispatcher created the temporary group on the MCPTT server of the primary MCPTT system.

6. The constituent groups of the temporary group may belong to MCPTT servers of the partner MCPTT systems.

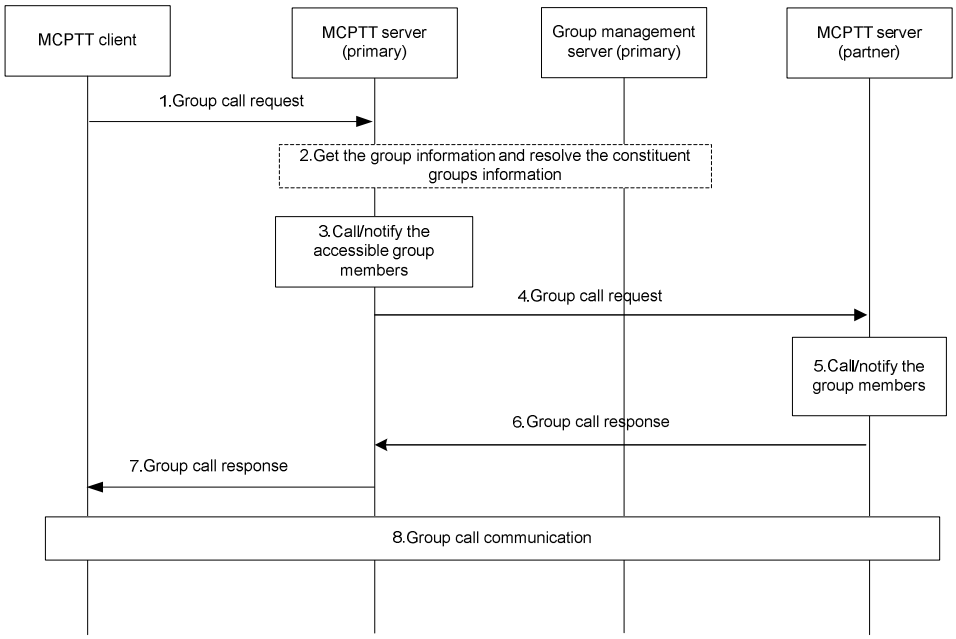

Figure 10.6.2.4.1.1.1-1: Group call setup involving temporary groups from multiple MCPTT systems (originating)

1. The affiliated MCPTT user via MCPTT client initiates a group call with a group id. A group call request message with the group id is routed to the MCPTT server of the primary MCPTT system, which owns the group and is where the authorized MCPTT user/dispatcher created the temporary group. If the group call is for a temporary group formed by the group regroup procedure, the group id will be a temporary group ID.

2. The MCPTT server of the primary MCPTT system gets the group information (either from group management server or itself) including the constituent MCPTT groups' identities, accessible group members list of the constituent groups, and other related data.

3. The MCPTT server of the primary MCPTT system initiates directly a call request to the accessible group members using the detailed user information and/or location information. The group members upon receipt of the call request may accept or reject the call. Alternatively, the MCPTT server of the primary MCPTT system notifies the group members via a notification message containing the group id and/or the group call session identity information. Upon receipt of the notification message, the group members may perform a late call entry.

4. The MCPTT server of the primary MCPTT system may not have access to group members' information of the constituent group belonging to the partner MCPTT system. For such group members, the MCPTT server of the primary MCPTT system initiates a group call request message to the MCPTT server of the partner MCPTT system with the target group's group id information.

5. The MCPTT server of the partner MCPTT system further initiates a call request or call notification to the constituent group's members as described in step 3.

6. The MCPTT server of the partner MCPTT system provides a group call response to the MCPTT server of the primary MCPTT system with success or failure result and/or detailed reason information in case of failure.

7. The MCPTT server of the primary MCPTT system provides a group call response message to the MCPTT client of the affiliated MCPTT user upon receiving responses to the call requests sent to members of primary and partner MCPTT systems. The group call response message will consist of the success or failure result and/or detailed reason information in case of failure.

NOTE: The group call response message is triggered depending on the conditions to proceed with the call.

8. Upon successful call setup completion a group call is established for the group members from constituent groups of multiple MCPTT servers.

10.6.2.4.1.1.2 Group call setup procedure – terminating side

The procedure in figure 10.6.2.4.1.1.2-1 illustrates the terminating side group call involving groups from multiple MCPTT systems. It considers the scenario for group hierarchies and temporary groups formed by group regroup. The protocol followed may be SIP.

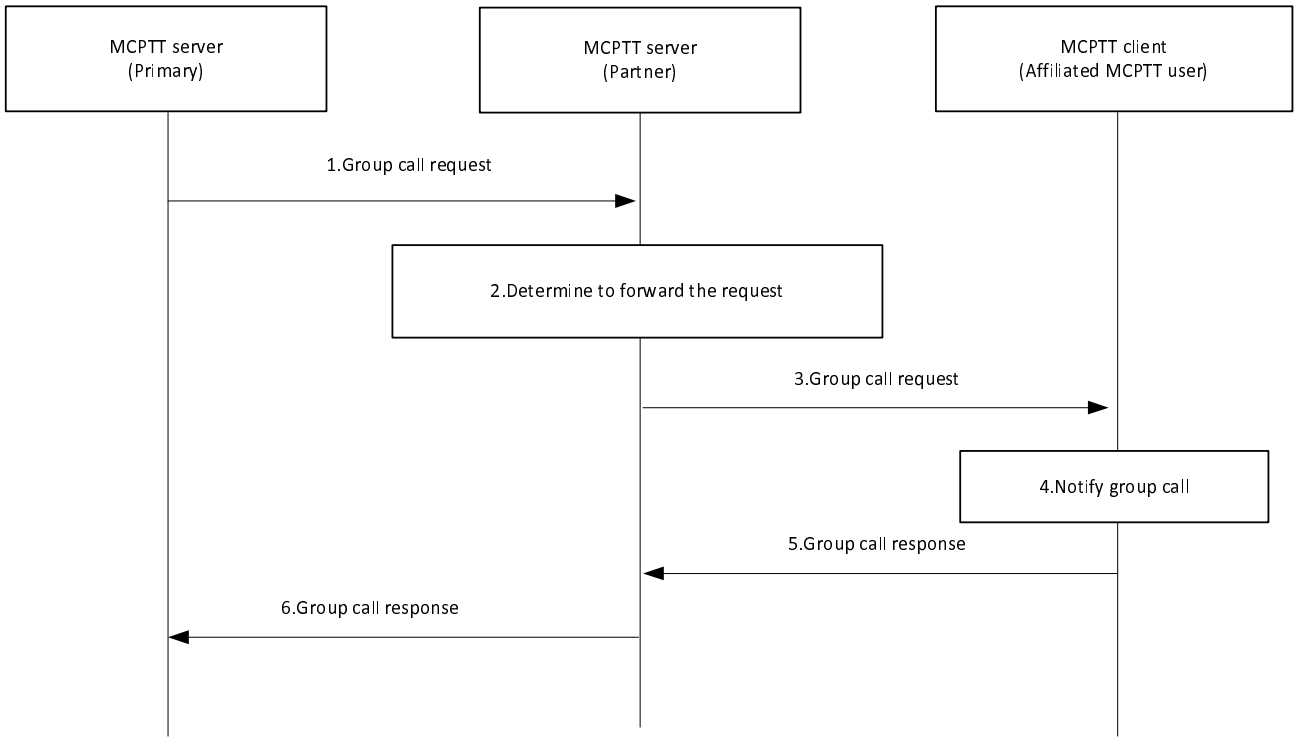

Figure 10.6.2.4.1.1.2-1: Group call involving groups from multiple MCPTT systems (terminating)

1. The MCPTT server of the primary MCPTT system sends the group call request message to the MCPTT server(s) of the partner MCPTT system.

2. The MCPTT server of the partner MCPTT system determines whether to forward the group call request message to the MCPTT client(s) based on the user affiliation.

3. The MCPTT server of the partner MCPTT system forwards the group call request message to MCPTT client(s). The MCPTT server indicates whether acknowledgement is required for the call.

4. The MCPTT user is notified about the incoming MCPTT group call.

5. The receiving MCPTT client(s) accept the group call request and a group call response message is sent to the MCPTT server of the partner MCPTT system. This response may contain an acknowledgement. The conditions for sending acknowledgement may be based on configuration.

6. The MCPTT server of the partner MCPTT system forwards the group call response message to the MCPTT server of the primary MCPTT system (i.e. group hosting MCPTT server for the group call involving groups from multiple MCPTT systems).

10.6.2.4.1.2 Group call release

The procedure focuses on the case where the group host MCPTT server releases an ongoing MCPTT group call for all the participants of that group call involving groups from multiple MCPTT systems, since at least one of the release conditions are met e.g., due to hang time expiry, last participant leaving, second last participant leaving, initiator leaving, or minimum number of affiliated MCPTT group members are not present.

NOTE: The scenario of MCPTT user leaving the group call is not considered in this procedure.

Figure 10.6.2.4.1.2-1 illustrates the procedure for the MCPTT server releasing an ongoing MCPTT group call involving groups from multiple MCPTT systems.

Pre-conditions:

1. The MCPTT server of the primary MCPTT system is controlling the group call involving groups from multiple MCPTT systems.

2. The MCPTT client 1 belongs to group of the MCPTT server of the primary MCPTT system and the MCPTT client 2 and client 3 belong to the groups of the MCPTT server of the partner MCPTT system.

3. The MCPTT users on MCPTT client 1, client 2 and client 3 are already part of the ongoing group call (e.g., as a result of group call setup involving groups from multiple MCPTT systems).

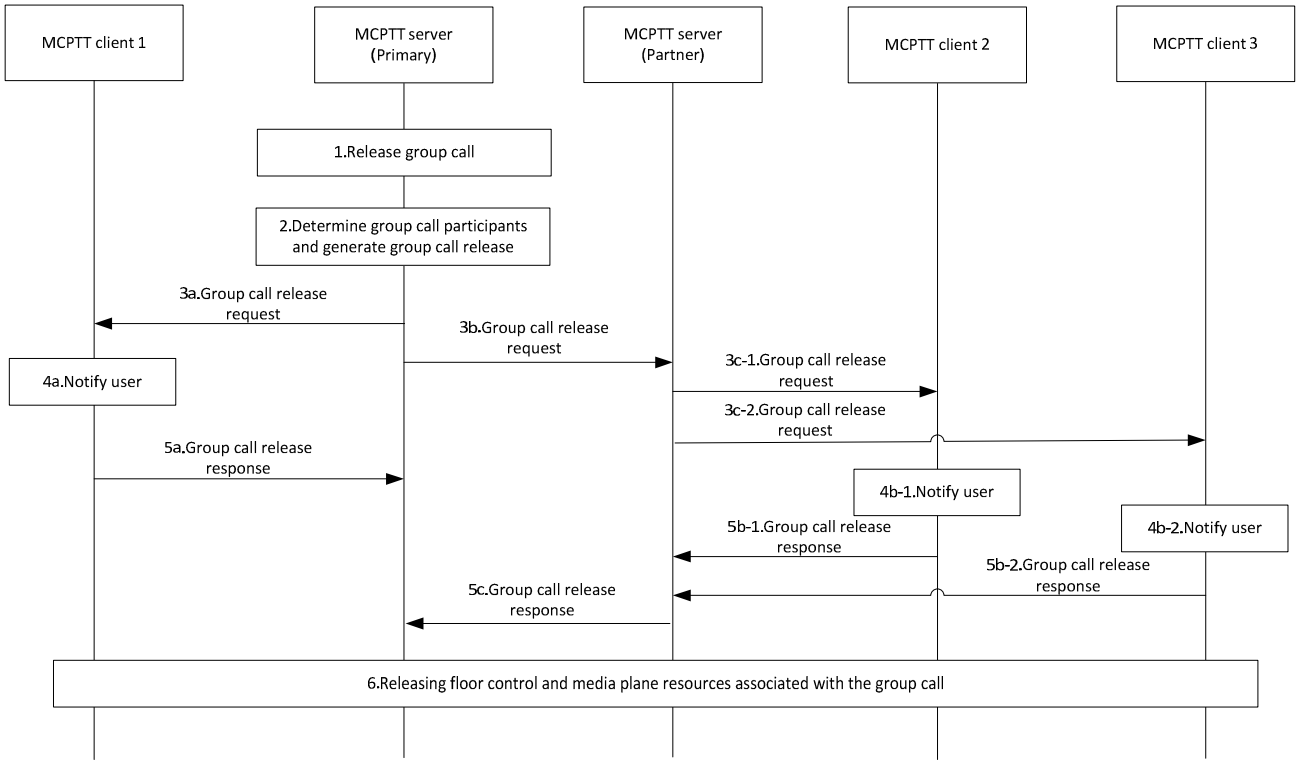

Figure 10.6.2.4.1.2-1: Group call release involving groups from multiple MCPTT systems

1. The MCPTT server of primary MCPTT system would like to release the MCPTT group call which is ongoing e.g., due to hang timer expiry, last participant leaving, second last participant leaving, initiator leaving, or minimum number of affiliated MCPTT group members are not present.

2. The MCPTT server of the primary MCPTT system identifies the participants of the ongoing group call and generates group call release message to release ongoing session.

3. The MCPTT server of the primary MCPTT system initiates a group call release request message via SIP core towards each accessible participant of the ongoing group call (3a). The MCPTT server of the primary MCPTT system may not have access to group members' information of the constituent group belonging to a partner MCPTT system. For such group members, the MCPTT server of the primary MCPTT system initiates a group call release request message (3b) to the MCPTT server(s) of the partner MCPTT system(s) with the target group's group id information. The MCPTT server(s) of the partner MCPTT system(s) further initiate group call release request messages (3c-1, 3c-2) to its group's users.

4. The MCPTT users are notified about the release of the group call.

5. The MCPTT client(s) receiving the group call release request messages provide group call release response to the MCPTT server of the primary MCPTT system. The MCPTT client(s) of the MCPTT users belonging to partner MCPTT system(s) route their responses via the MCPTT server(s) of the partner MCPTT system(s).

6. The MCPTT client 1, client 2 and client 3 have successfully released the floor control and media plane resources associated with the group call that is released.

10.6.2.4.2 Group call for temporary group formed by group regroup procedure involving multiple MCPTT systems via trusted mode

Figure 10.6.2.4.2-1 illustrates a group call involving a temporary group formed by group regroup from multiple MCPTT systems. The protocol followed may be SIP.

Pre-conditions:

1. The security aspects of sharing the user information between primary and partner MCPTT systems shall be governed as per the service provider agreement between them. In this case, we consider the partner MCPTT system shares their users' information to the primary MCPTT system.

2. The MCPTT user belongs to an MCPTT group hosted by the primary MCPTT system.

3. A temporary group is formed by authorized MCPTT user/dispatcher by the group regroup procedure (subclause 10.4.4.2) and identified via a temporary group ID.

4. The MCPTT group members of the constituent MCPTT groups belonging to the temporary group are affiliated to participate in a group call for the temporary group.

5. The authorized MCPTT user/dispatcher created the temporary group on the MCPTT server of the primary MCPTT system.

6. The constituent groups of the temporary group may belong to MCPTT servers of the partner MCPTT systems.

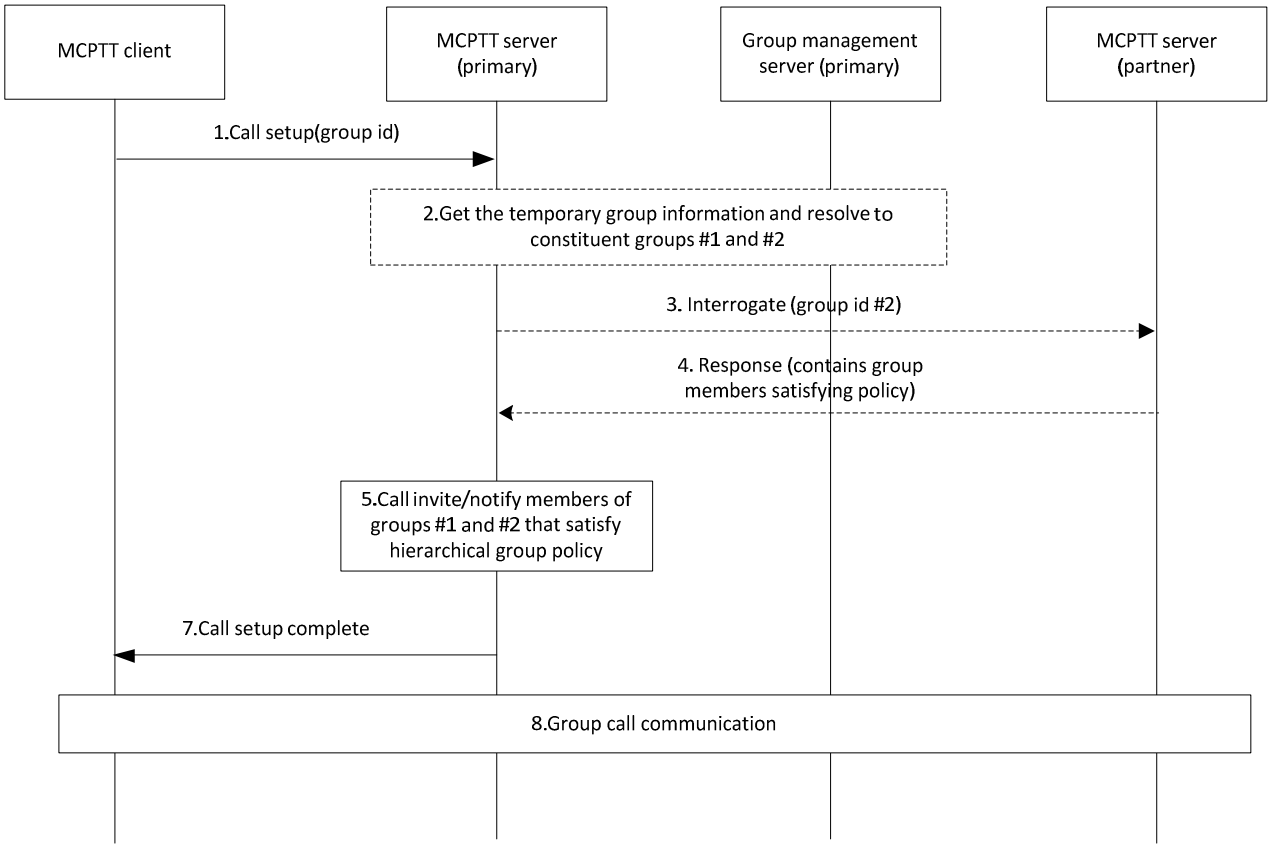

Figure 10.6.2.4.2-1: Group call involving temporary group formed by group regroup from multiple MCPTT systems

1. The affiliated MCPTT user via MCPTT client initiates a group call with a group id. A call setup message with the group id is routed to the MCPTT server of the primary MCPTT system, which owns the temporary group formed by group regroup procedure, and is also where the authorized MCPTT user/dispatcher has created the temporary group. The group id will be a temporary group identity.

2. The MCPTT server of the primary MCPTT system gets the group information (either from group management server or itself) including the constituent MCPTT groups' identities, and other related data.

3. The MCPTT server of the primary MCPTT system may interrogate the MCPTT server of the partner MCPTT system for the affiliated group 2 members.

4. The MCPTT server of the partner MCPTT system responds with a list of the affiliated group members of group 2.

NOTE 1: Steps 3 and 4 do not occur if the constituent groups' information is available and up to date at primary MCPTT system due to the procedure for temporary group formation as defined in subclause 10.4.4.2.

5. The MCPTT server of the primary MCPTT system verifies the commencement policies of the temporary group, and initiates a call invitation or call notification to the affiliated members of groups 1 and 2.

6. The MCPTT server of the primary MCPTT system provides a call setup complete response via a call setup complete message to the MCPTT UE of authorized MCPTT user/dispatcher upon receiving responses to the call invitations sent to members of primary and partner MCPTT systems. The call setup complete response will consist of the success or failure result and/or detailed reason information in case of failure.

8. Upon successful call setup completion a group call is established for the group members belonging to constituent groups of multiple MCPTT systems.

NOTE 2: MCPTT clients are generally aware that their (constituent) groups have been regrouped (e.g., see subclause 10.1.5.3); however, if not, the partner MCPTT server of the constituent group can also respond to a group call request with a redirection response, such as "moved temporarily" that includes the group URI of the temporary group formed by group regroup procedure.

10.6.2.4.3 Group call for an MCPTT group defined in the partner MCPTT system

10.6.2.4.3.1 Group call setup procedure – initiating side

Figure 10.6.2.4.3.1-1 illustrates the group call setup procedure for an MCPTT group defined in the partner MCPTT system.

Pre-conditions:

1. MCPTT group is defined on the group management server which is located in the partner MCPTT system with MCPTT users affiliated to that group.
2. The members of the MCPTT group defined in partner MCPTT system belong to different MCPTT systems.

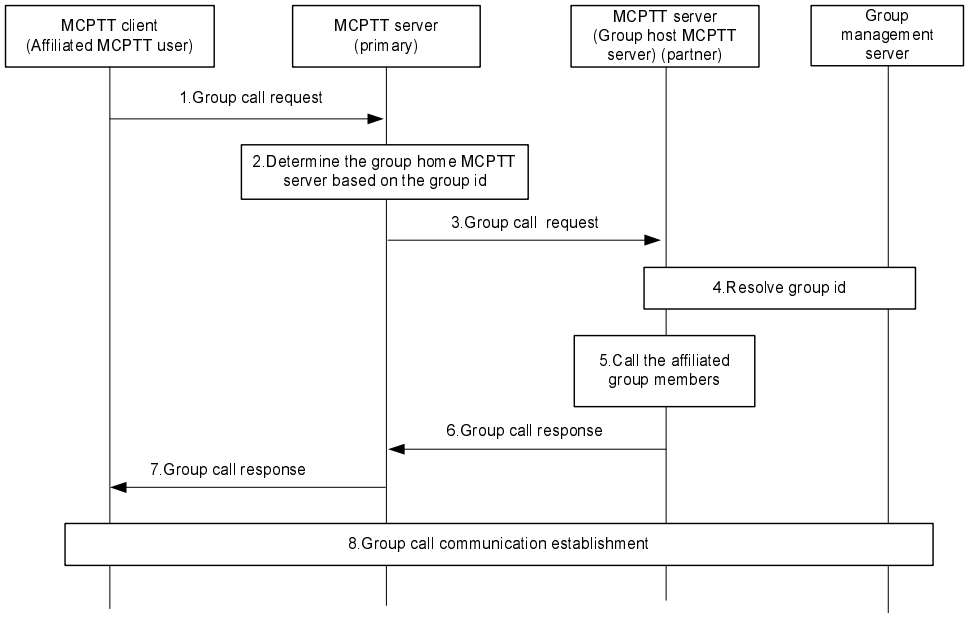

Figure 10.6.2.4.3.1-1: Group call for an MCPTT group defined in partner MCPTT system (initiating)

1. The affiliated MCPTT user via MCPTT client initiates a group call with a group id. A group call request message with the group id is routed to the MCPTT server of the primary MCPTT system.
2. The MCPTT server of the primary MCPTT system determines the group home MCPTT server where the MCPTT group is defined.
3. The MCPTT server of the primary MCPTT system forwards the group call request to the MCPTT server of the partner MCPTT system which owns the group and is where the authorized MCPTT user/dispatcher created the temporary group.
4. The MCPTT server of the partner MCPTT system checks whether the user of MCPTT client is authorized for initiating the group call for the selected group. If authorized, it resolves the group id to determine the members of that group and their affiliation status, based on the information from group management server.
5. The MCPTT server of the partner MCPTT system initiates a call request to the group's affiliated members.
6. The MCPTT server of the partner MCPTT system provides a group call response message to the MCPTT server of the primary MCPTT system of the MCPTT client. The group call response message will consist of the success or failure result and/or detailed reason information in case of failure.
7. The MCPTT server of the primary MCPTT system forwards the group call response message to the MCPTT client.

8 Upon successful call setup completion a group call is established for the group members.

10.6.2.4.3.2 Group call setup – terminating side

The procedure described in figure 10.6.2.4.3.2-1 is used for group call setup when acknowledgement is required from at least some of the call recipients.

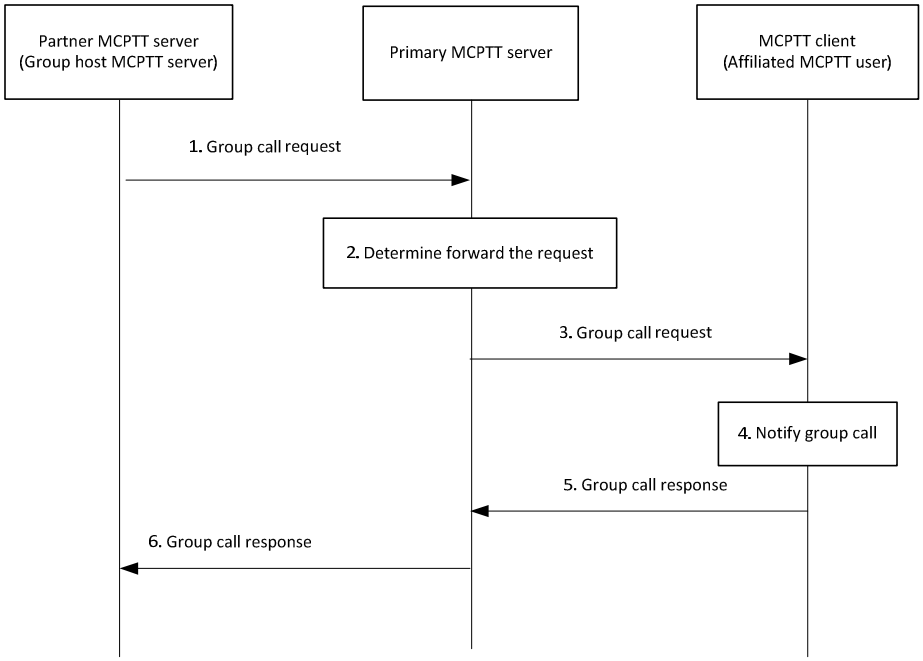

Figure 10.6.2.4.3.2-1: Group call for an MCPTT group defined in partner MCPTT system (terminating)

1. MCPTT server of the partner MCPTT system sends the group call request message towards to the MCPTT server of the primary MCPTT system of the MCPTT client.
2. The MCPTT server of the primary MCPTT system determines whether to forward the group call request message to the MCPTT client based on the user subscription.
3. The MCPTT server of the primary MCPTT system forwards the group call request message to MCPTT client. The MCPTT server indicates whether acknowledgement is required for the call.
4. MCPTT user is notified about the incoming group call.
5. The receiving MCPTT client accepts the group call and a response message is sent to the MCPTT server of the primary MCPTT system. This response may contain an acknowledgement. The conditions for sending acknowledgement may be based on configuration.
6. The MCPTT server of the primary MCPTT system forwards the response message to the MCPTT server of the partner MCPTT system (i.e. group hosting MCPTT server).

10.6.2.4.4 Merging of groups involving multiple MCPTT systems

Figure 10.6.2.4.4-1 below illustrates the merging of MCPTT clients in a newly formed temporary group with active group calls.

Pre-conditions:

1. The temporary group consists of group 1, which is hosted by the primary MCPTT system, and group 2, which is hosted by the partner MCPTT system.
2. Both group 1 and group 2 have active calls.
3. The group management client of the authorized MCPTT user belongs to the primary MCPTT system.

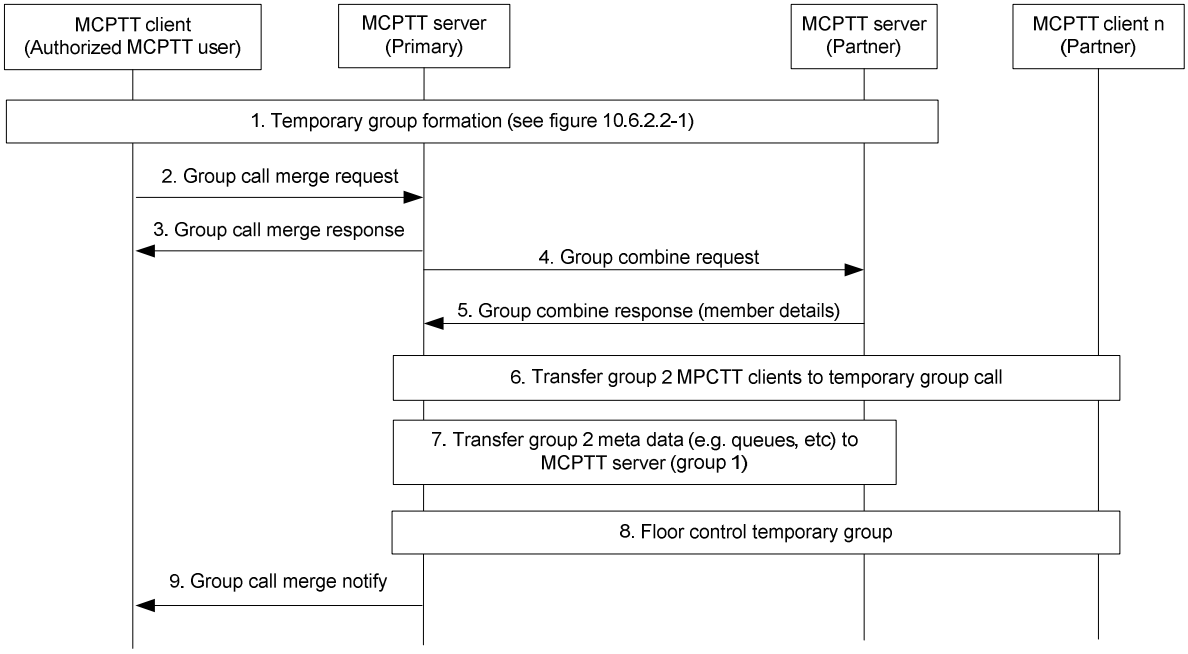

Figure 10.6.2.4.4-1: Merging of groups involving multiple MCPTT systems

1. The temporary group formation - group regrouping involving multiple MCPTT systems, according to subclause 10.4.4.2 takes place.
2. The MCPTT client of the authorized MCPTT user requests group call merge operation to MCPTT server hosting group 1. The identities of the groups being combined are included in this message.
3. The MCPTT server (primary) responds with an OK response.
4. The MCPTT server (primary) sends a group combine request to the MCPTT server (partner) that is hosting group 2.
5. The MCPTT server (partner) responds with a list members of group 2 and an indication of which members are affiliated and which are active in the call.
6. The MCPTT server (primary) contacts the active members of group 2 inviting them to join the temporary group call.
7. The MCPTT server (partner) transfers group 2's floor status data (including pending requests and queue positions) to the primary MCPTT server and combines this with the group 1's floor status data in order to create the temporary group's floor status data.
8. The MCPTT server (primary) performs floor control for the temporary group.
9. The MCPTT server (primary) notifies the MCPTT client of the authorised MCPTT user that the active calls have been merged.

NOTE: The MCPTT server in primary system revokes and queues floor given to one of the two talkers based on the arbitration result for the temporary group.

10.6.2.5 Broadcast group call

10.6.2.5.1 General

A broadcast group call is a special group call where the initiating MCPTT user expects no response from the other MCPTT users, so that when his transmission is complete, so is the call.

10.6.2.5.2 Common broadcast group call procedure

The group-broadcast group and the regrouped group are similar in structure (a collection of groups). Similarly the user-broadcast group and the pre-arranged group (a collection of users) are similar in structure. Only the call originator can transmit media during the broadcast group call and the broadcast group call is released when the transmission is complete.

Figure 10.6.2.5.2-1 illustrates the common procedure both for group-broadcast group call and user-broadcast group call.

Pre-conditions:

1. MCPTT client 1 and MCPTT client 2 are members of a group-broadcast group/user-broadcast group.

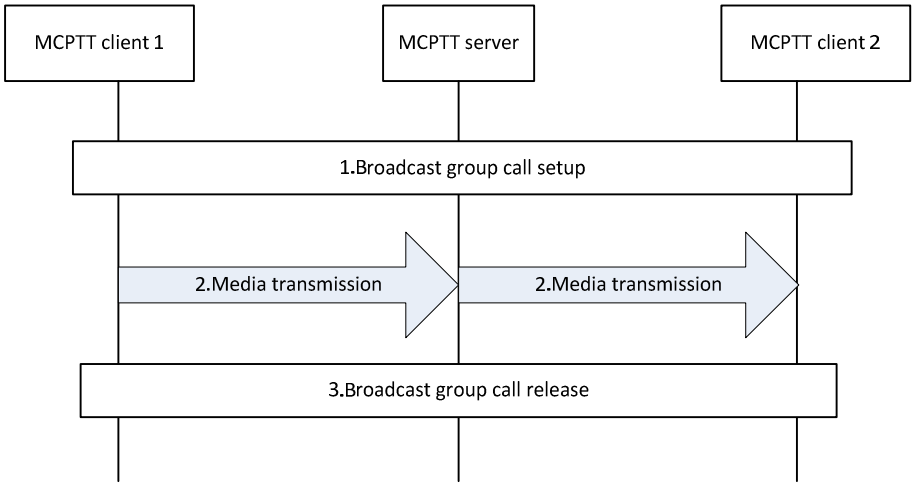

Figure 10.6.2.5.2-1: Broadcast group call

1. MCPTT user at MCPTT client 1 initiates the broadcast group call setup procedure with the indication of broadcast group call. The signalling procedure is identical to the group call setup as described in subclause 10.6.2 with the inclusion of the parameter for broadcast group call indicator.

2. MCPTT client 1 starts to transmit media.

NOTE 1: Only the call originating MCPTT user is allowed to transmit media on broadcast group call.

NOTE 2: A broadcast group call transmitted on a user-broadcast group has priority over group calls involving users within the user hierarchy. A broadcast group call transmitted on a group-broadcast group has priority over group calls on its subordinate groups.

3. If the media transmission from call originating MCPTT user is complete, the broadcast group call is released.

10.6.2.5.3 Temporary group – broadcast group call procedure

Figure 10.6.2.5.3-1 illustrates the procedure for temporary group-broadcast group call procedure. The protocol used may be SIP.

Pre-conditions:

1. The security aspects of sharing the user information between primary and partner MCPTT systems shall be governed as per the service provider agreement between them. In this case, we consider the partner MCPTT system does not share their users' information to the primary MCPTT system.

2. The authorized MCPTT user/dispatcher belongs to the primary MCPTT system.

3. The MCPTT server of the primary MCPTT system is where the authorized MCPTT user/dispatcher created the temporary group.

4. Other groups in the temporary group – broadcast group may belong to partner MCPTT systems.

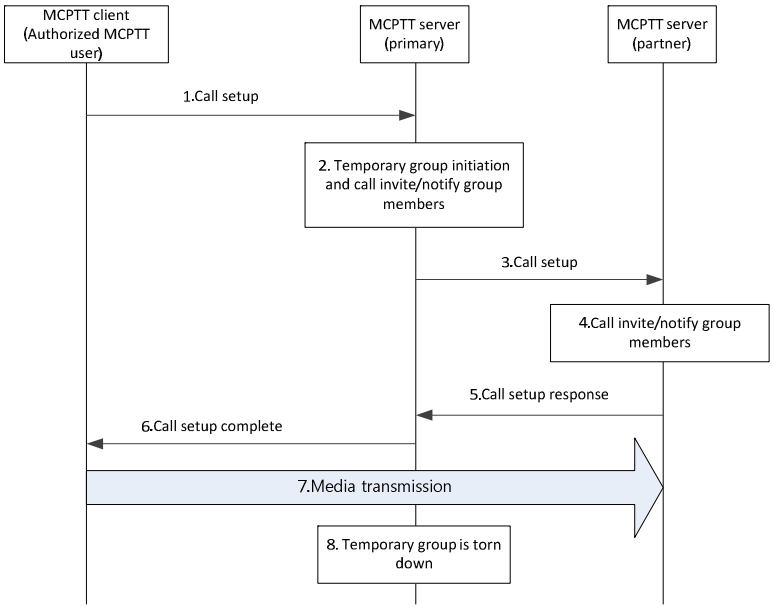

Figure 10.6.2.5.3-1: Temporary group – broadcast group call

1. The MCPTT client of authorized user initiates a group call with multiple groups from primary and partner MCPTT systems. A call setup message with the MCPTT group IDs (group id1, group id2) is routed to the MCPTT server of the primary MCPTT system, which is where the authorized MCPTT user/dispatcher created the temporary group.

2. The MCPTT server of the primary MCPTT system forms the temporary group with the groups' information received. It resolves the MCPTT group IDs and identifies the appropriate MCPTT server responsible for the groups. It further triggers a temporary group – broadcast group call via a call invite message to the affiliated group members of group id1 of the MCPTT server of the primary MCPTT system.

NOTE 1: The temporary group information is not notified to the group members of the constituent groups.

3. A call setup message is further initiated with the MCPTT server of the partner MCPTT system for group id2.

4. Upon receiving the call setup message from the MCPTT server of the primary MCPTT system, the MCPTT server of the partner MCPTT system initiates a call invitation to their affiliated group members. The group members upon receipt of the invitation may accept or reject the call. Alternatively, the MCPTT server of the partner MCPTT system notifies the group members via a notification message containing the group call session identity information. Upon receipt of the notification message, the group members may perform a late call entry.

5. The MCPTT server of the partner MCPTT system provides a call setup response to the MCPTT server of the primary MCPTT system with success or failure result and/or detailed reason information in case of failure.

6. The MCPTT server of the primary MCPTT system provides a call setup complete response via a call setup complete message to the MCPTT client of the authorized MCPTT user upon receiving response to the corresponding call setup with the MCPTT server of the partner MCPTT system. The call setup complete response will consist of the success or failure result and/or detailed reason information in case of failure.

NOTE 2: The call setup complete message is triggered depending on the conditions to proceed with the call.

7. Upon successful call setup completion, a group call is established amongst the multiple group members from primary and partner MCPTT systems. The call originating MCPTT user starts transmitting media to other group call participants.

NOTE 3: Only the call originating MCPTT user is allowed to transmit media on broadcast group call.

NOTE 4: A broadcast group call transmitted on a temporary group-broadcast group has priority over group calls on its subordinate groups.

8. At the completion of the media transmission, the broadcast group call is released, and the temporary group – broadcast group is torn down.

10.6.2.5.3 User broadcast group

10.6.2.6 Emergency and imminent peril procedures

10.6.2.6.1 MCPTT emergency group call

10.6.2.6.1.1 MCPTT emergency group call commencement

The procedure focuses on the case where an MCPTT client is initiating an MCPTT emergency group call with the affiliated MCPTT members of that MCPTT group. An MCPTT client in the MCPTT emergency state gains elevated access privilege for all of the MCPTT user's mission critical applications.

Procedures in figure 10.6.2.6.1.1-1 are the signalling control plane procedures for the MCPTT client initiating establishment of an MCPTT emergency group call with an MCPTT group i.e., MCPTT users on MCPTT client 1, MCPTT client 2 and MCPTT client 3 belong to the same MCPTT group which is defined on MCPTT group management server.

NOTE 1: For simplicity, a single MCPTT server is shown in place of a user home MCPTT server and a group hosting MCPTT server.

Pre-conditions:

1. The MCPTT group is previously defined on the group management server with MCPTT client 2 and MCPTT client 3 affiliated to that MCPTT group.

2. All members of the MCPTT group belong to the same MCPTT system.

3. The initiating MCPTT client 1 has been provisioned with an MCPTT group that has been designated via provisioning as the MCPTT emergency group.

NOTE 2: Alternatively, the client could have been provisioned for emergency behaviour on the selected group.

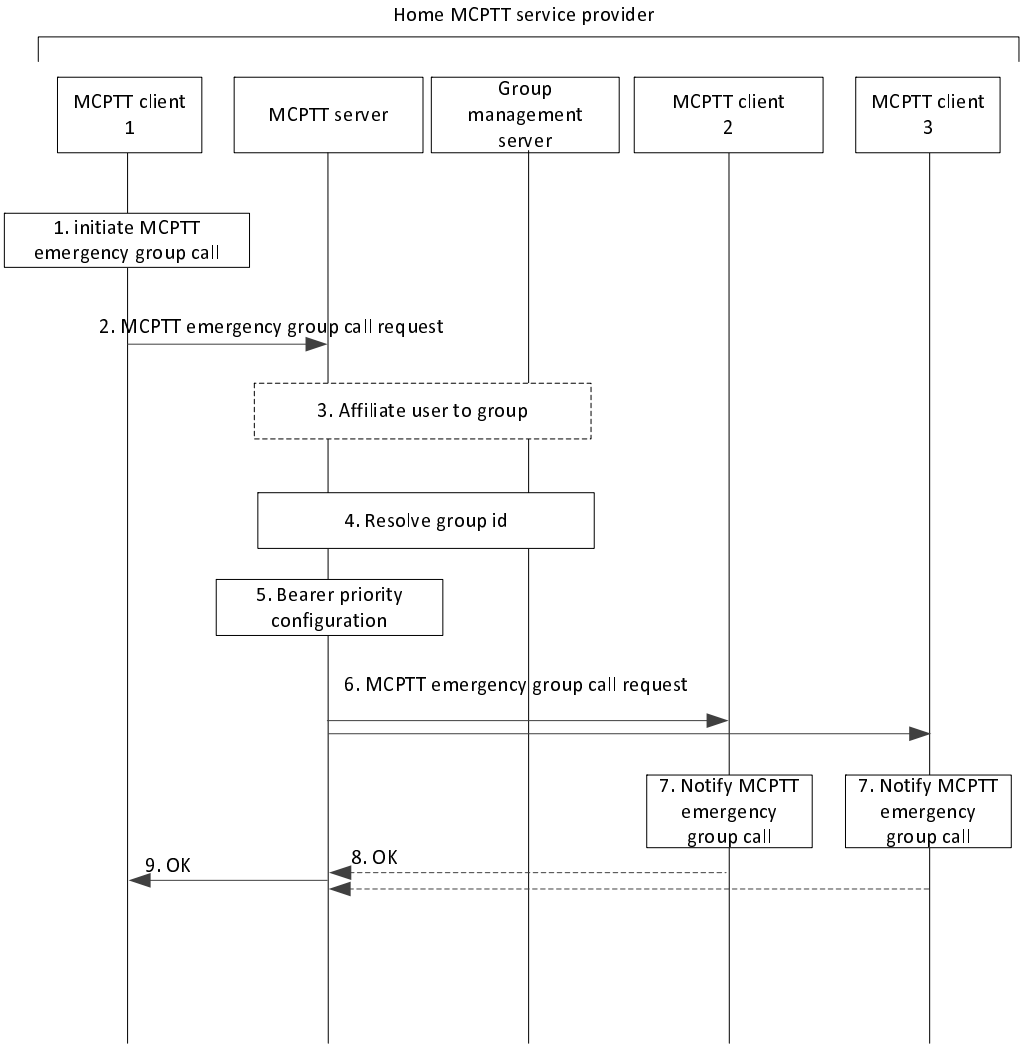

Figure 10.6.2.6.1.1-1: MCPTT emergency group call

1. The user at the MCPTT client 1 initiates an MCPTT emergency group call. MCPTT client 1 sets its MCPTT emergency state. The MCPTT emergency state is retained until explicitly cancelled.

2. MCPTT client 1 sends an MCPTT group call request towards the MCPTT server. The request contains an indication of the MCPTT emergency. The MCPTT server records the identity of the MCPTT user that initiated the MCPTT emergency group call until the MCPTT emergency is cancelled. Once an MCPTT emergency call has been initiated, the MCPTT group is considered to be in an in-progress emergency state until cancelled. If configured to send an MCPTT emergency alert when initiating an MCPTT emergency group call, the request also contains an indication that an MCPTT emergency alert is to be initiated. The request may contain an indication of an implicit floor request.

3. The MCPTT server implicitly affiliates the client to the emergency group if the client is not already affiliated.

4. MCPTT server checks whether the MCPTT user of MCPTT client 1 is authorized for initiation of MCPTT emergency calls on the indicated MCPTT group, and if authorized, it resolves the MCPTT group ID to determine the members of that MCPTT group and their affiliation status, based on the information from group management server.

5. The MCPTT server configures the priority of the underlying bearers for all participants in the MCPTT group.

NOTE 3: Successive calls during the MCPTT group's in-progress emergency state will all receive the adjusted bearer priority.

6. MCPTT server sends the MCPTT emergency group call request towards the MCPTT clients of each of those affiliated MCPTT group members. The request contains an indication of the in-progress emergency. The request

contains an indication of an MCPTT emergency alert if the request from the originator indicated MCPTT emergency alert.

7. MCPTT users are notified of the incoming MCPTT group call.

8. The receiving MCPTT clients acknowledge the MCPTT emergency group call request to the MCPTT server. For a multicast call, these acknowledgements are not sent.

9. The MCPTT server informs the MCPTT client 1 about the successful MCPTT emergency call establishment.

NOTE 4: Step 9 can occur at any time following step 5, and prior to step 10 depending on the conditions to proceed with the call.

MCPTT client 1, MCPTT client 2 and MCPTT client 3 have successfully established media plane for communication. MCPTT floor participant 1, floor participant 2 and floor participant 3 exchange floor control information e.g., MCPTT client 1 receives the floor granted information over the established media plane, while the other MCPTT client's receive floor taken information. MCPTT client 1 indicates to the MCPTT user that the floor is available to send media, while the other MCPTT clients in the MCPTT emergency group call will be receiving that media. MCPTT client 1 can override other clients in the call except those that are also in the MCPTT emergency state.

10.6.2.6.1.2 MCPTT group call upgraded to an MCPTT emergency group call

The procedure focuses on the case where an authorized MCPTT user is upgrading an MCPTT group call to an MCPTT emergency group call while the MCPTT group call is already in progress.

Procedures in figure 10.6.2.6.1.2-1 are the signalling control plane procedures for the MCPTT client upgrading an MCPTT group call on an MCPTT group to an MCPTT emergency group call.

NOTE 1: For simplicity, a single MCPTT server is shown in place of a user home MCPTT server and a group hosting MCPTT server.

Pre-conditions:

1. The MCPTT group is previously defined on the group management server with MCPTT client 2 and MCPTT client 3 affiliated to that MCPTT group.

2. All members of the MCPTT group belong to the same MCPTT system.

3. An MCPTT group call is already in progress.

4. The initiating MCPTT client 1 has been configured to send an MCPTT emergency alert when upgrading an MCPTT emergency group call.

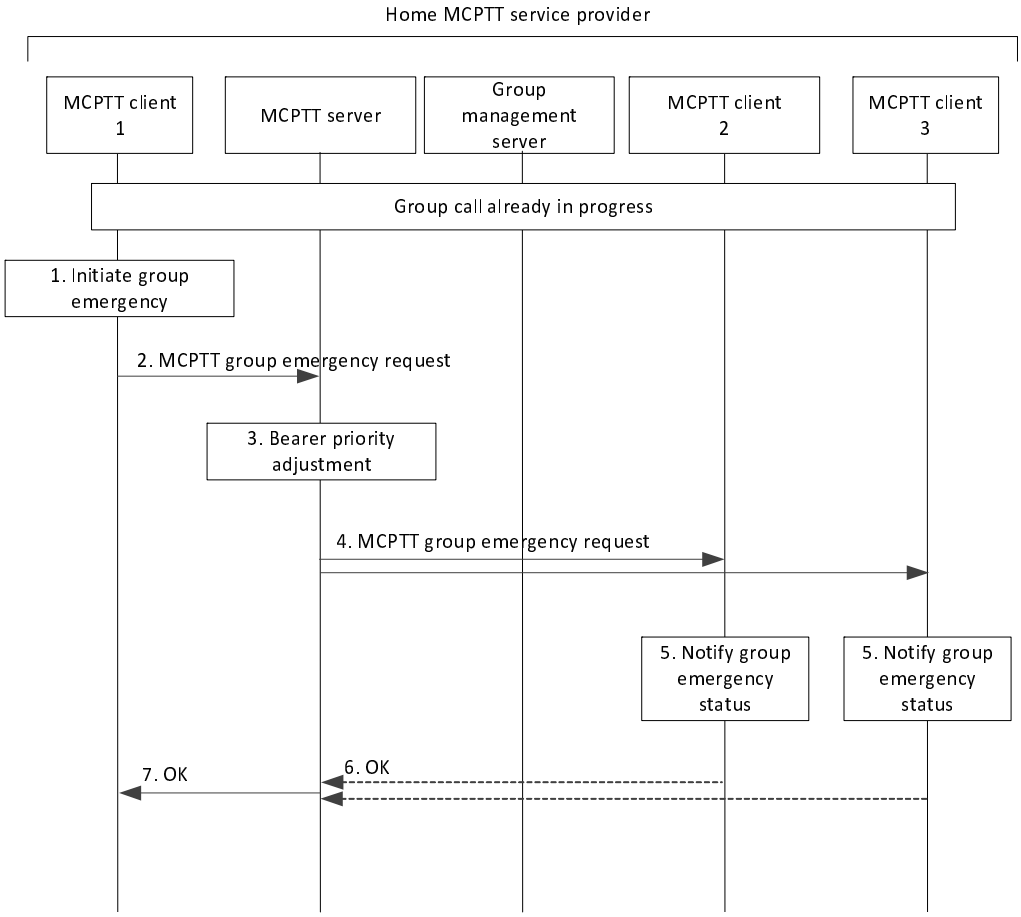

Figure 10.6.2.6.1.2-1: MCPTT group call upgraded to an MCPTT emergency group call

1. The MCPTT user at MCPTT client 1 initiates a group emergency. MCPTT client 1 sets its MCPTT emergency state. The MCPTT emergency state is retained until explicitly cancelled.

2. MCPTT client 1 requests the MCPTT server to upgrade the MCPTT group to an in-progress emergency state by sending an MCPTT group emergency request. If configured to send an MCPTT alert when initiating an MCPTT emergency upgrade, the request also contains an indication that an MCPTT alert is to be initiated. The request may contain an indication of an implicit floor request.

3. The MCPTT server adjusts the priority of the underlying bearer for all participants in the MCPTT group.

4. MCPTT server sends the MCPTT group emergency request towards the MCPTT clients of each of those affiliated MCPTT group members. The request contains an indication of an MCPTT emergency alert if the request from the originator indicated MCPTT emergency alert.

5. MCPTT users are notified of the in-progress emergency state of the MCPTT group.

6. The receiving MCPTT clients acknowledge the MCPTT group emergency request to the MCPTT server. For a multicast call, these acknowledgements are not sent.

7. The MCPTT server confirms the upgrade request to MCPTT client 1. If the MCPTT emergency request contained an implicit floor request, the OK message contains the result of the implicit floor request.

NOTE 2: Step 7 can occur at any time following step 3, and prior to step 8 depending on the conditions to proceed with the call.

MCPTT client 1, MCPTT client 2 and MCPTT client 3 continue with the MCPTT group call, which has been transformed into an MCPTT emergency group call. MCPTT client 1 can override other clients in the call except those that are also in the MCPTT emergency state.

10.6.2.6.1.3 MCPTT group emergency cancel

The procedure focuses on the case where an MCPTT client cancels an MCPTT group's in-progress emergency.

Procedures in figure 10.6.2.6.1.3-1 are the signalling control plane procedures for the MCPTT client cancelling an in-progress emergency.

NOTE 1: For simplicity, a single MCPTT server is shown in place of a user home MCPTT server and a group hosting MCPTT server.

NOTE 2: The end of the MCPTT emergency group call does not cancel the MCPTT group's in-progress emergency state. It is explicitly cancelled by an authorized user.

Pre-conditions:

1. The MCPTT group is previously defined on the group management server with MCPTT client 2 and MCPTT client 3 affiliated to that MCPTT group.
2. All members of the MCPTT group belong to the same MCPTT system.
3. MCPTT group members have been notified about the in-progress emergency.
4. The MCPTT group is in the in-progress emergency state and has prioritized bearer support.
5. MCPTT client 1 previously initiated the in-progress emergency.

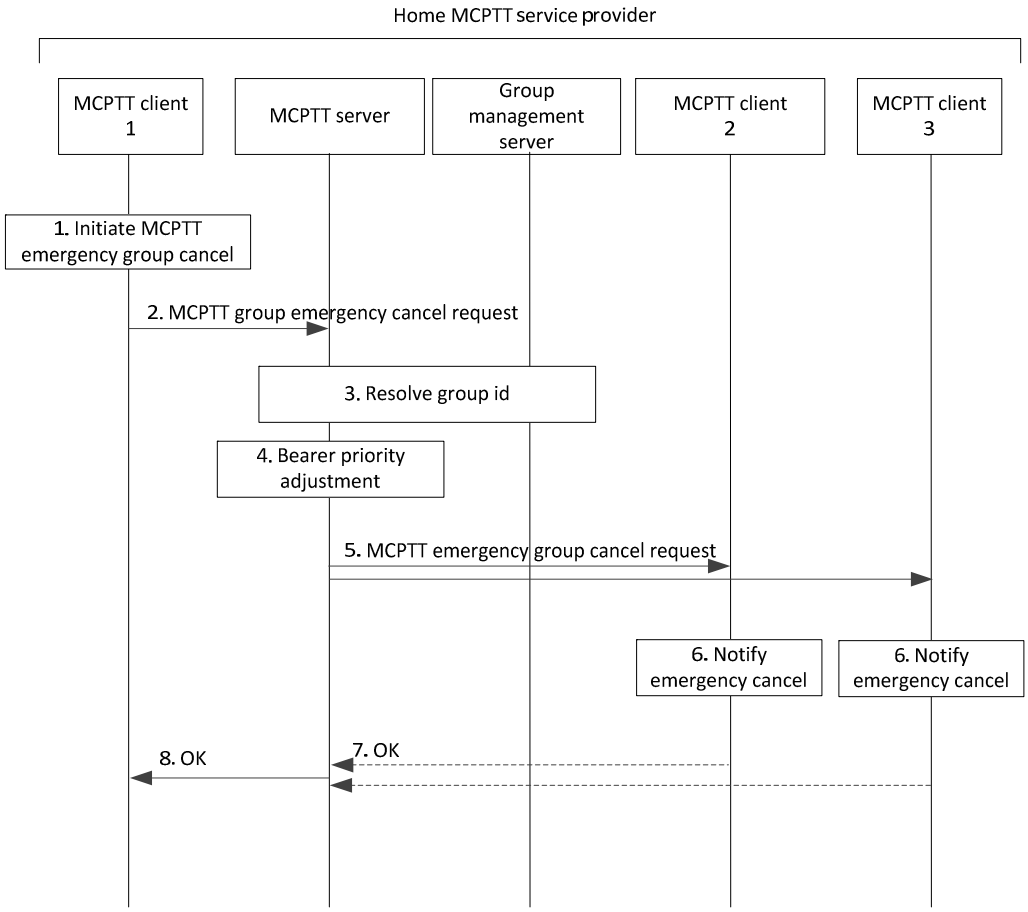

Figure 10.6.2.6.1.3-1: MCPTT emergency group cancel

1. The user at the MCPTT client 1 initiates an MCPTT emergency group cancel.

NOTE 3: An MCPTT user authorized to cancel in-progress emergencies on the MCPTT group can also be authorised to cancel the MCPTT emergency alert in addition to the initiator. However, only the initiator can cancel the initiator's local MCPTT emergency state.

2. MCPTT client 1 sends an MCPTT emergency group cancel request to the MCPTT server.

NOTE 4: When MCPTT emergency alerts are in effect together with an MCPTT emergency group condition on the same MCPTT group, the MCPTT emergency alert can, under some circumstances be cancelled at the same time. In that case, the MCPTT emergency group cancel request carries an indication that the alert is also being cancelled.

3. MCPTT server resolves the MCPTT group ID to determine the members of that MCPTT group and their affiliation status, based upon the information from group management server.

4. The MCPTT server adjusts the priority of the underlying bearer; priority treatment is no longer required. The MCPTT server cancels/resets the emergency in-progress state of the MCPTT group.

5. The MCPTT server sends an MCPTT emergency group cancel request to the MCPTT group members.

6. MCPTT group members are notified of the MCPTT emergency cancel.

7. The receiving MCPTT group members acknowledge the MCPTT emergency cancel to the MCPTT server. For a multicast call scenario, these acknowledgements are not sent.

8. The MCPTT server confirms the MCPTT emergency group cancel to MCPTT client 1. MCPTT client 1 resets its local emergency status since it is the one requesting the MCPTT emergency group cancel.

NOTE 5: Step 8 can occur at any time following step 4, depending on the conditions to proceed with the call.

10.6.2.6.2 MCPTT imminent peril group call

10.6.2.6.2.1 MCPTT imminent peril group call commencement

The procedure focuses on the case where an authorized MCPTT user is initiating an imminent peril group call for communicating with the affiliated MCPTT members of that MCPTT group. This procedure will gain elevated access privilege for the MCPTT client if it is not already in that state. The access privilege for other applications will not necessarily be affected.

Procedures in figure 10.6.2.6.2.1-1 are the signalling control plane procedures for the MCPTT client initiating establishment of an imminent peril group call with an MCPTT group i.e., MCPTT users on MCPTT client 1, MCPTT client 2 and MCPTT client 3 belong to the same MCPTT group which is defined on MCPTT group management server.

Pre-conditions:

1. The MCPTT group is previously defined on the group management server with MCPTT client 2 and MCPTT client 3 affiliated to that MCPTT group.

2. All members of the MCPTT group belong to the same MCPTT system.

3. The initiating MCPTT client 1 has been provisioned with an MCPTT group that has been designated in the provisioning to be used for imminent peril communications.

NOTE 1: Alternatively, the client could have been provisioned for imminent peril behaviour on the selected group.

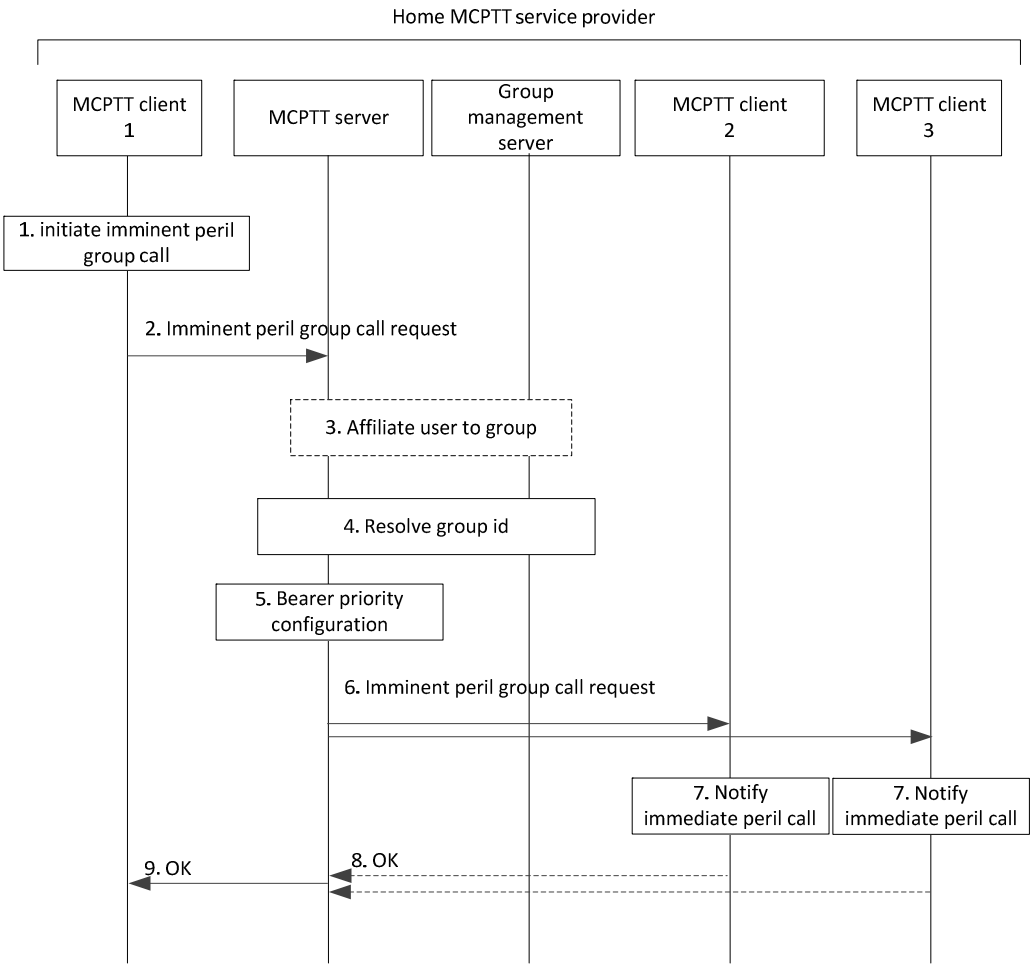

Figure 10.6.2.6.2.1-1: MCPTT imminent peril group call

1. The user at the MCPTT client 1 initiates an imminent peril group call.

2. MCPTT client 1 sends an MCPTT imminent peril group call request towards the MCPTT server. The request contains an indication of the in-progress imminent peril. The MCPTT server records the identity of the MCPTT user that initiated the imminent peril group call until the in-progress imminent peril state is cancelled. Once an imminent peril group call has been initiated, the MCPTT group is considered to be in an in-progress imminent peril state until cancelled. The request may contain an indication of an implicit floor request.

3. The MCPTT server implicitly affiliates the client to the imminent peril group if the client is not already affiliated.

4. MCPTT server checks whether the MCPTT user of MCPTT client 1 is authorized for initiation of imminent peril group calls on the indicated MCPTT group, and if authorized, it resolves the MCPTT group ID to determine the members of that MCPTT group and their affiliation status, based on the information from group management server.

5. The MCPTT server configures the priority of the underlying bearers for all participants in the MCPTT group.

NOTE 2: Successive calls during the in-progress imminent peril state will all receive the adjusted bearer priority.

6. MCPTT server sends the imminent peril group call request towards the MCPTT clients of each of those affiliated MCPTT group members. The request contains an indication of the in-progress imminent peril.

7. MCPTT users are notified of the incoming imminent peril call.

8. The receiving MCPTT clients acknowledge the imminent peril call request to the MCPTT server. For a multicast call, these acknowledgements are not set.

9. The MCPTT server informs the MCPTT client 1 about the successful imminent peril call establishment. If the MCPTT imminent peril request contained an implicit floor request, the OK message contains the result of the implicit floor request.

NOTE 3: Step 9 can occur at any time following step 5, and prior to step 10 depending on the conditions to proceed with the imminent peril call.

MCPTT client 1, MCPTT client 2 and MCPTT client 3 have successfully established media plane for communication. MCPTT floor participant 1, floor participant 2 and floor participant 3 exchange floor control information e.g., MCPTT client 1 receives the floor granted information over the established media plane, while the other MCPTT clients receive floor taken information. MCPTT client 1 indicates to the MCPTT user that the floor is available to send media, while the other MCPTT clients in the imminent peril call will be receiving that media.

10.6.2.6.2.2 Imminent peril group call upgrade

The procedure focuses on the case where an authorized MCPTT user is upgrading an MCPTT group call to an imminent peril group call while the MCPTT group call is already in progress.

Procedures in figure 10.6.2.6.2.2-1 are the signalling control plane procedures for the MCPTT client upgrading an MCPTT group call on an MCPTT group to an imminent peril group call.

Pre-conditions:

1. The MCPTT group is previously defined on the group management server with MCPTT client 1, MCPTT client 2 and MCPTT client 3 affiliated to that MCPTT group.

2. All members of the MCPTT group belong to the same MCPTT system.

3. An MCPTT group call is already in progress.

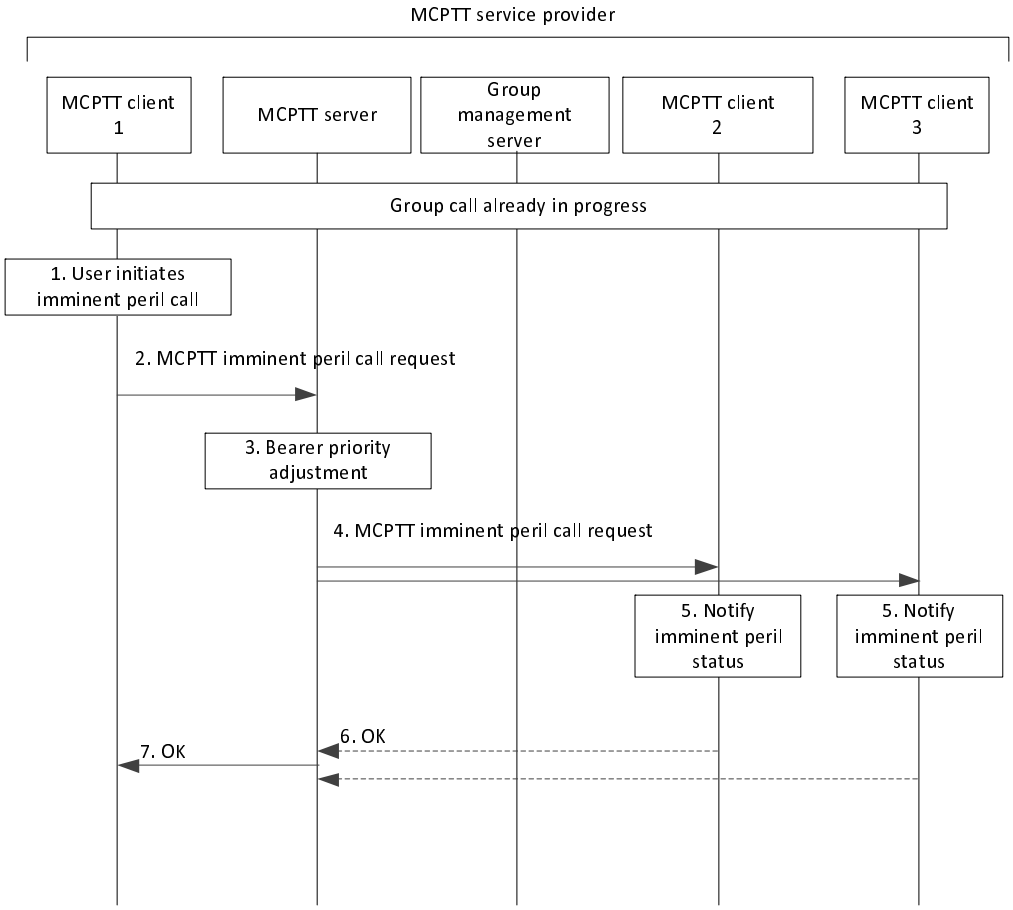

Figure 10.6.2.6.2.2-1: MCPTT group call upgrade to an imminent peril group call

1. The MCPTT user at MCPTT client 1 initiates an imminent peril call.
2. MCPTT client 1 requests the MCPTT server to upgrade the MCPTT group to an in-progress imminent peril state by sending an MCPTT imminent peril call request. The request may contain an indication of an implicit floor request.
3. The MCPTT server adjusts the priority of the underlying bearer for all participants in the MCPTT group.
4. MCPTT server sends the MCPTT imminent peril call request towards the MCPTT clients of each of those affiliated MCPTT group members.
5. MCPTT users are notified of the in-progress imminent peril state of the MCPTT group.
6. The receiving MCPTT clients acknowledge the MCPTT imminent peril call request to the MCPTT server. For a multicast call, these acknowledgements are not set.
7. The MCPTT server confirms the upgrade request to MCPTT client 1. If the MCPTT imminent peril call request contained an implicit floor request, the OK message contains the result of the implicit floor request.

NOTE: Step 7 can occur at any time following step 4, and prior to step 8 depending on the conditions to proceed with the call.

MCPTT client 1, MCPTT client 2 and MCPTT client 3 continue with the MCPTT group call, which has been transformed into an imminent peril group call.

10.6.2.6.2.3 MCPTT imminent peril group call cancel

The procedure focuses on the case where an authorized MCPTT user cancels an MCPTT group's in-progress imminent peril state.

Procedures in figure 10.6.2.6.2.3-1 are the signalling control plane procedures for the MCPTT client cancelling an MCPTT group's in-progress imminent peril state.

NOTE 1: The end of the imminent peril call does not cancel the MCPTT group's in-progress imminent peril state. It is explicitly cancelled by an authorized user.

Pre-conditions:

1. The MCPTT group is previously defined on the group management server with MCPTT client 1, MCPTT client 2 and MCPTT client 3 affiliated to that MCPTT group.
2. All members of the MCPTT group belong to the same MCPTT system.
3. The MCPTT group is an in-progress imminent peril state and has prioritized bearer support.
4. MCPTT group members have been notified about the MCPTT group's in-progress imminent peril state.
5. MCPTT client 1 previously initiated the in-progress imminent peril.

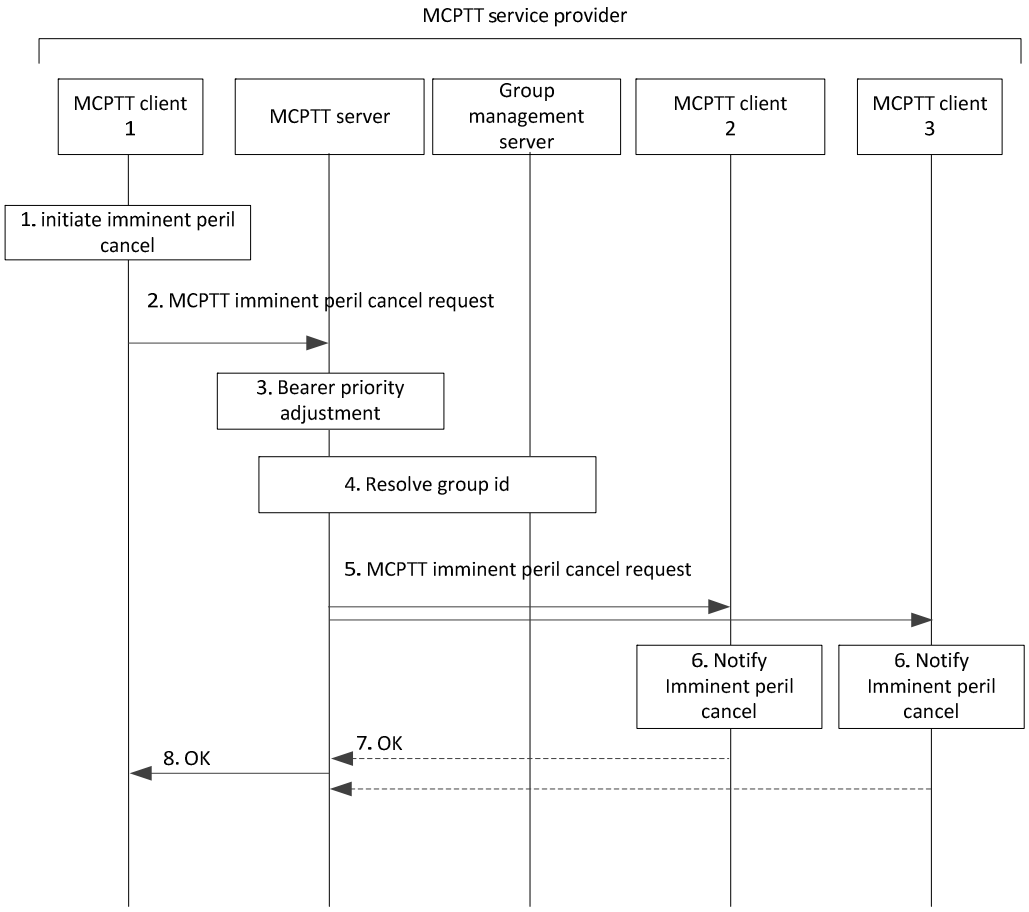

Figure 10.6.2.6.2.3-1: MCPTT imminent peril group call cancel

1. The user at the MCPTT client 1 initiates an imminent peril cancel.
2. MCPTT client 1 sends an MCPTT imminent peril cancel request to the MCPTT server.
3. The MCPTT server adjusts the priority of the underlying bearer; priority treatment is no longer required. The MCPTT server cancels/resets the in-progress imminent peril state.
4. MCPTT server resolves the MCPTT group ID to determine the members of that MCPTT group and their affiliation status, based upon the information from group management server.

5. The MCPTT server sends an MCPTT imminent peril cancel request to the MCPTT group members.

6. MCPTT group members are notified of the in-progress imminent peril cancel.

7. The receiving MCPTT group members acknowledge the in-progress MCPTT imminent peril cancel request to the MCPTT server. For a multicast scenario, these acknowledgements are not set.

8. The MCPTT server confirms the MCPTT imminent peril cancel request to MCPTT client 1.

NOTE 2: Step 8 can occur at any time following step 4, depending on the conditions to proceed with the call.

10.6.2.6.3 MCPTT emergency alert

10.6.2.6.3.1 MCPTT emergency alert initiation

The procedure focuses on the case where an MCPTT client is initiating an MCPTT emergency alert unicast signalling for communicating the alert with the affiliated MCPTT members of that MCPTT group. An MCPTT client in the MCPTT emergency state gains elevated access privilege for all of the MCPTT user's mission critical applications. This procedure will place the MCPTT client in the MCPTT emergency state if the MCPTT client is not already in that state.

Procedures in figure 10.6.2.6.3.1-1 are the signalling control plane procedures for the MCPTT client initiating an MCPTT emergency alert with an MCPTT group i.e., MCPTT users on MCPTT client 1, MCPTT client 2 and MCPTT client 3 belong to the same MCPTT group which is defined on MCPTT group management server.

NOTE 1: For simplicity, a single MCPTT server is shown in place of a user home MCPTT server and a group hosting MCPTT server.

Pre-conditions:

1. The MCPTT group is previously defined on the group management server with MCPTT client 2 and MCPTT client 3 affiliated to that MCPTT group.

2. All members of the MCPTT group belong to the same MCPTT system.

3. The initiating MCPTT client 1 is affiliated with one or more MCPTT groups.

4. The initiating MCPTT client 1 has been provisioned with an MCPTT group designated as the MCPTT emergency group.

NOTE 2: Alternatively, the client could have been provisioned for emergency behaviour on the currently selected group.

5. The initiating MCPTT client 1 may not have carried out an explicit affiliation procedure with the MCPTT group designated as the MCPTT emergency group.

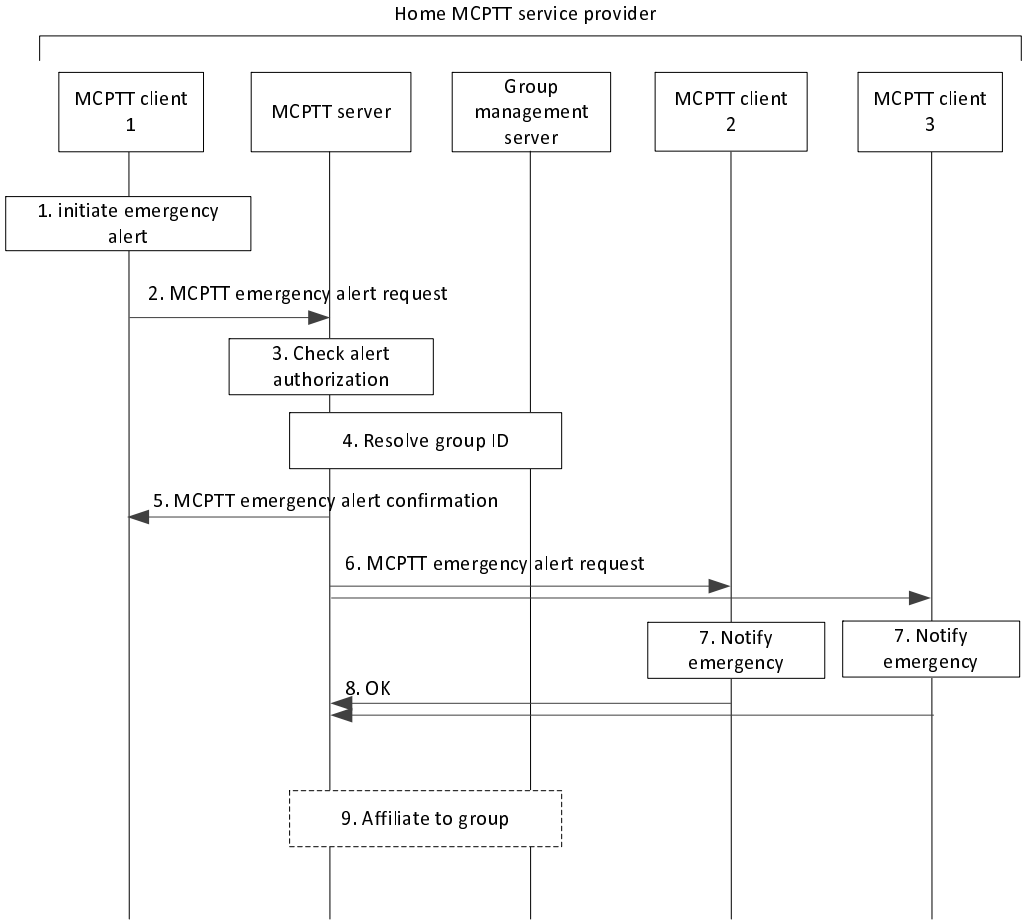

Figure 10.6.2.6.3.1-1 MCPTT emergency alert

1. The user at the MCPTT client 1 initiates an MCPTT emergency alert. MCPTT client 1 sets its MCPTT emergency state. The MCPTT emergency state is retained by the MCPTT client until explicitly cancelled.

2. MCPTT client 1 requests the MCPTT server to send an MCPTT emergency alert request to the MCPTT group designated as the MCPTT emergency group.

3. MCPTT server checks whether the MCPTT user of MCPTT client 1 is authorized for initiation of MCPTT emergency alerts for the indicated MCPTT group.

4. MCPTT server resolves the MCPTT group ID to determine the members of that MCPTT group and their affiliation status, based on the information from group management server.

5. The MCPTT server confirms to MCPTT client 1 the MCPTT emergency alert request. MCPTT group calls made to this MCPTT group by the MCPTT client 1 will be sent as emergency calls until the in-progress emergency state on the MCPTT client 1 is cancelled.

6. The MCPTT server sends an MCPTT emergency alert request towards the MCPTT clients of each of those affiliated MCPTT group members. The MCPTT emergency alert request message shall contain the following information: Location, User ID and group ID (i.e., MCPTT user's selected MCPTT group or dedicated MCPTT emergency group, as per MCPTT group configuration) and the MCPTT user's mission critical organization name.

7. MCPTT users are notified of the MCPTT emergency.

8. The receiving MCPTT clients acknowledge the MCPTT emergency alert to the MCPTT server.

9. The MCPTT server implicitly affiliates the client to the emergency group if the client is not already affiliated.

NOTE 3: Sending the emergency alert without making a request to also start an emergency call does not put the group into the ongoing emergency condition.

NOTE 4: Sending the emergency alert does not put the other UEs in the group into an emergency state.

NOTE 5: The MCPTT client 1 need not initiate a group call. For example, the MCPTT client can be configured to only allow alerts or the MCPTT user can choose not to make an MCPTT emergency group call.

10.6.2.6.3.2 MCPTT emergency state cancel

The procedure focuses on the case where an MCPTT client has initiated an MCPTT emergency alert and entered the emergency state, and wishes to cancel this state, informing the MCPTT server and other group members of this cancellation. By doing so, the MCPTT client may also request the cancellation of the ongoing emergency condition in the group.

Procedures in figure 10.6.2.6.3.2-1 are the signalling control plane procedures for the MCPTT client cancelling an MCPTT emergency state with an MCPTT group i.e., MCPTT users on MCPTT client 1, MCPTT client 2 and MCPTT client 3 belong to the same MCPTT group which is defined on MCPTT group management server.

NOTE 1: For simplicity, a single MCPTT server is shown in place of a user home MCPTT server and a group hosting MCPTT server.

Pre-conditions:

1. The MCPTT client 1 had previously successfully initiated an MCPTT emergency alert.
2. The MCPTT client 1 is still in the emergency state.
3. The initiating MCPTT client 1 has affiliated with the MCPTT group designated as the MCPTT emergency group.

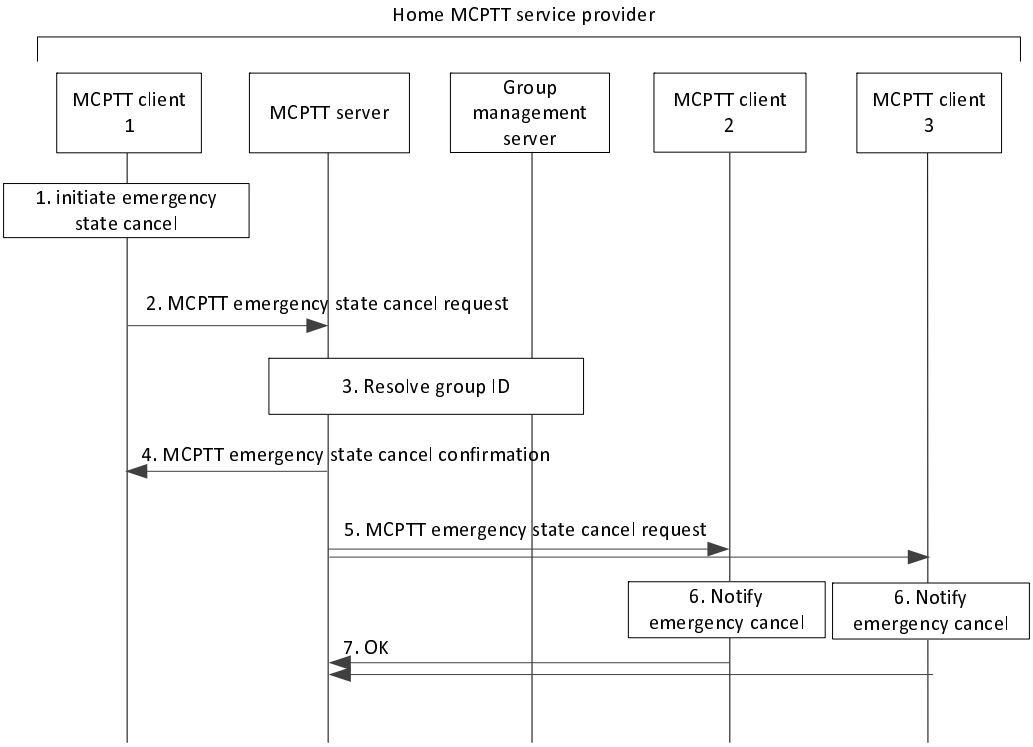

Figure 10.6.2.6.3.2-1 MCPTT emergency state cancel

1. The user at the MCPTT client 1 initiates an MCPTT emergency state cancel.

NOTE 2: The MCPTT emergency state cancel request carries an indication to also request that the in-progress emergency is to be cancelled. The MCPTT server can accept or deny the request to cancel the ongoing emergency condition of the group as a whole, separately from accepting or denying the request to cancel the emergency state at MCPTT client 1. Additionally, an authorized user can cancel either or both the ongoing emergency condition of the group and the initiator's local MCPTT emergency state.

2. MCPTT client 1 requests the MCPTT server to send an MCPTT emergency state cancel to the MCPTT group to which MCPTT client 1 had previously sent the emergency alert.

3. MCPTT server resolves the MCPTT group ID to determine the members of that MCPTT group and their affiliation status, based on the information from group management server.

4. The MCPTT server confirms to MCPTT client 1 the MCPTT emergency state cancel request. MCPTT client 1 resets its emergency state.

5. The MCPTT server sends an MCPTT emergency state cancel request towards the MCPTT clients of each of those affiliated MCPTT group members.

7. MCPTT users are notified of the MCPTT emergency state cancellation of MCPTT client 1.

8. The receiving MCPTT clients acknowledge the MCPTT emergency state cancel to the MCPTT server. For a multicast call scenario, these acknowledgements are not sent.

10.6.3 Off-network group call

10.6.3.1 General

Off-network group calls can use pre-defined configuration information provided to MCPTT clients prior to the off-network group call or configuration information that is transmitted to MCPTT clients during group call setup or late entry procedures.

If off-network group configuration information is pre-defined (e.g. codec to be used) and provided to the MCPTT clients prior to the off-network group call (e.g. as part of group metadata), the MCPTT client will be able to participate in the off-network group call without needing to follow the group call setup or late joining procedures as they will be able to receive the media and signalling without the need for the announcement or invitation.

If off-network group configuration information is not pre-defined or provided, call parameters need to be transmitted to MCPTT clients via group call announcement or invitation.

10.6.3.2 Information flows for group call in off-network

10.6.3.2.1 Group call announcement

Table 10.6.3.2.1-1 describes the information flow for the group call announcement from the MCPTT client to other MCPTT clients.

Table 10.6.3.2.1-1: Group call announcement

Information Element	Status	Description
MCPTT ID	M	The identity of the calling party
MCPTT group ID	M	The MCPTT group on which the call is to be conducted
Media type	M	Type of the media to be used for the call
Media codec	M	The media codec to be used for the call
Multi-cast port	M	Multicast port number for media
Bandwidth	M	Bearer bandwidth to be used for the call
Floor control port number	M	Port number for floor control protocol
Announcement period	M	Period of the group call announcement
Encryption parameters	O	Encryption parameters to be used for the call, if the call is to be encrypted
Confirm mode indicator	O	Indicates whether the MCPTT group call is to be confirmed
Emergency indicator	O	Indicates that the MCPTT group call is an MCPTT emergency call
Imminent peril indicator	O	Indicates that the MCPTT group call is an MCPTT imminent peril call

10.6.3.2.2 MCPTT upgrade to emergency call

Table 10.6.3.2.2-1 describes the information flow for the MCPTT upgrade to emergency from the MCPTT client to other MCPTT clients.

Table 10.6.3.2.2-1: MCPTT upgrade to emergency call

Information Element	Status	Description
MCPTT ID	M	The identity of the upgrading party
MCPTT group ID	M	The MCPTT group ID on which the call is to be conducted

10.6.3.2.3 MCPTT emergency group cancel

Table 10.6.3.2.3-1 describes the information flow for the MCPTT upgrade to emergency request from the MCPTT client to other MCPTT clients.

Table 10.6.3.2.3-1: MCPTT emergency group cancel

Information Element	Status	Description
MCPTT ID	M	The identity of the cancelling party
MCPTT group ID	M	The MCPTT group ID of the call to be cancelled

10.6.3.2.4 Response

Table 10.6.3.2.4-1 describes the information flow for the response.

Table 10.6.3.2.4-1: Response

Information Element	Status	Description
MCPTT ID	M	The identity of the called party

10.6.3.2.5 MCPTT emergency alert request

Table 10.6.3.2.5-1 describes the information flow for the MCPTT emergency alert request from the MCPTT client to the other MCPTT clients.

Table 10.6.3.2.5-1: MCPTT emergency alert

Information Element	Status	Description
MCPTT ID	M	The identity of the alerting MCPTT user
Group ID	M	The MCPTT group ID with which the alert is associated
Location	O	The alerting client's location, if known
Organization name	M	The alerting user"s mission critical organization name

10.6.3.2.6 MCPTT emergency alert cancel

Table 10.6.3.2.6-1 describes the information flow for the MCPTT emergency alert cancel from the MCPTT client to other MCPTT clients.

Table 10.6.3.2.6-1: MCPTT emergency alert cancel

Information Element	Status	Description
MCPTT ID	M	The identity of the cancelling MCPTT user
MCPTT group ID	M	The MCPTT group ID with which the alert is associated

10.6.3.2.7 MCPTT upgrade to imminent peril call

Table 10.6.3.2.7-1 describes the information flow for the MCPTT upgrade to imminent peril from the MCPTT client to other MCPTT clients.

Table 10.6.3.2.7-1: MCPTT upgrade to imminent peril call

Information Element	Status	Description
MCPTT ID	M	The identity of the upgrading party
Group ID	M	The group identity of the group to be upgraded

10.6.3.2.8 MCPTT imminent peril group call cancel

Table 10.6.3.2.8-1 describes the information flow MCPTT imminent peril group call cancel from the MCPTT client to other MCPTT clients.

Table 10.6.3.2.8-1: MCPTT imminent peril group call cancel

Information Element	Status	Description
MCPTT ID	M	The identity of the cancelling party
Group ID	M	The group identity on which the imminent peril is to be cancelled

10.6.3.3 Group call setup

The flow in figure 10 6.3.3-1 illustrates the control plane procedures for MCPTT group call establishment for off-network. The procedure describes how an MCPTT client initiates an MCPTT group call with other MCPTT client within the off-network radio coverage and how the group call is established.

Pre-conditions:

- It is assumed that information for ProSe direct communications corresponding to the mappings of MCPTT group ID and ProSe Layer-2 Group ID (see subclause 8.1.3.2) are pre-configured;
- It is assumed that a multicast IP address and port for the call setup signalling are pre-configured;
- All messages exchanged between the MCPTT clients for the MCPTT group follows ProSe direct communications as defined in 3GPP TS 23.303 [8]; and
- The MCPTT users of MCPTT client 1, 2 and 3 belong to the same MCPTT group.

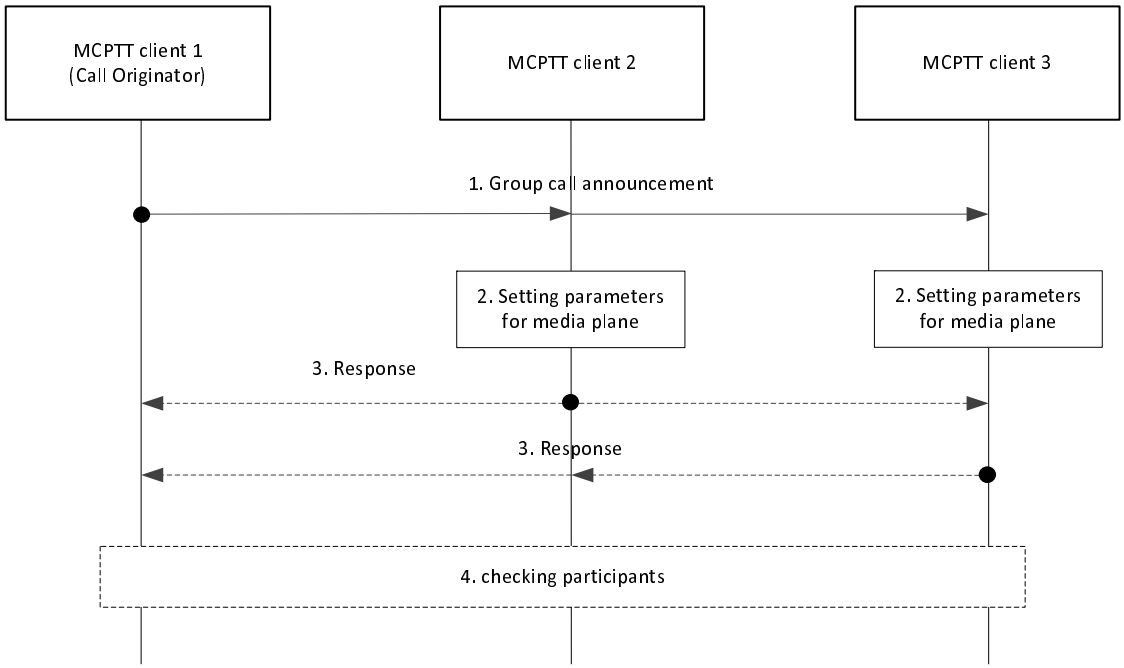

Figure 10.6.3.3-1: Off-network group call setup

1. MCPTT client 1 as the group call originator sends group call announcement message to the group. This message contains the following parameters such as MCPTT group ID, group call originator identity, media type, media codec, bandwidth, multicast port number for media, port number for floor control protocol, period of group call announcement, and any encryption key for the media encryption if needed, and optionally confirm mode indication.

NOTE 1: The group call announcement includes at least one common set of parameters and values for media transfer. Additional values per parameter will not be prohibited for the better user experience.

NOTE 2: By using the ProSe Layer-2 Group ID mapping with the MCPTT group ID, ProSe layer ensures that the messages sent for the corresponding MCPTT group are only received by its group's members.

2. MCPTT client 2, 3 join the group call. The MCPTT clients configure the parameters for media delivery by making use of the received parameters in group call announcement.

3. MCPTT client 2, 3 may send the response message to the group when the group call announcement from originator includes confirm mode indication. This message contains MCPTT ID.

4. MCPTT client 2, 3 recognize the group call originator through the group call announcement and MCPTT client 1 checks the participants of the group call through the received response message.

NOTE 3: Due to the movement of the participants (in and out of the radio coverage) during the off-network group call, the group call announcement message including parameters for media delivery is periodically sent.

NOTE 4: The participating MCPTT clients do not need to respond to the periodic group call announcement.

10.6.3.4 Passive join to group call

Figure 10 6.3.4-1 illustrates the control plane procedures for the passive MCPTT client to join the on-going MCPTT group call. The passive MCPTT client does not initiate to establish an MCPTT group call, but receives the group call announcement to be transferred periodically. When receiving the announcement message with parameters for media transfer, the passive MCPTT client configures the parameter to receive the voice and joins the announced MCPTT group call.

This procedure happens after the MCPTT group call is established. The group call announcement including the parameters for the media transfer has been performed periodically, in order for the MCPTT client later to join the MCPTT group call.

The MCPTT client 4 enters the coverage of the MCPTT group call lately.

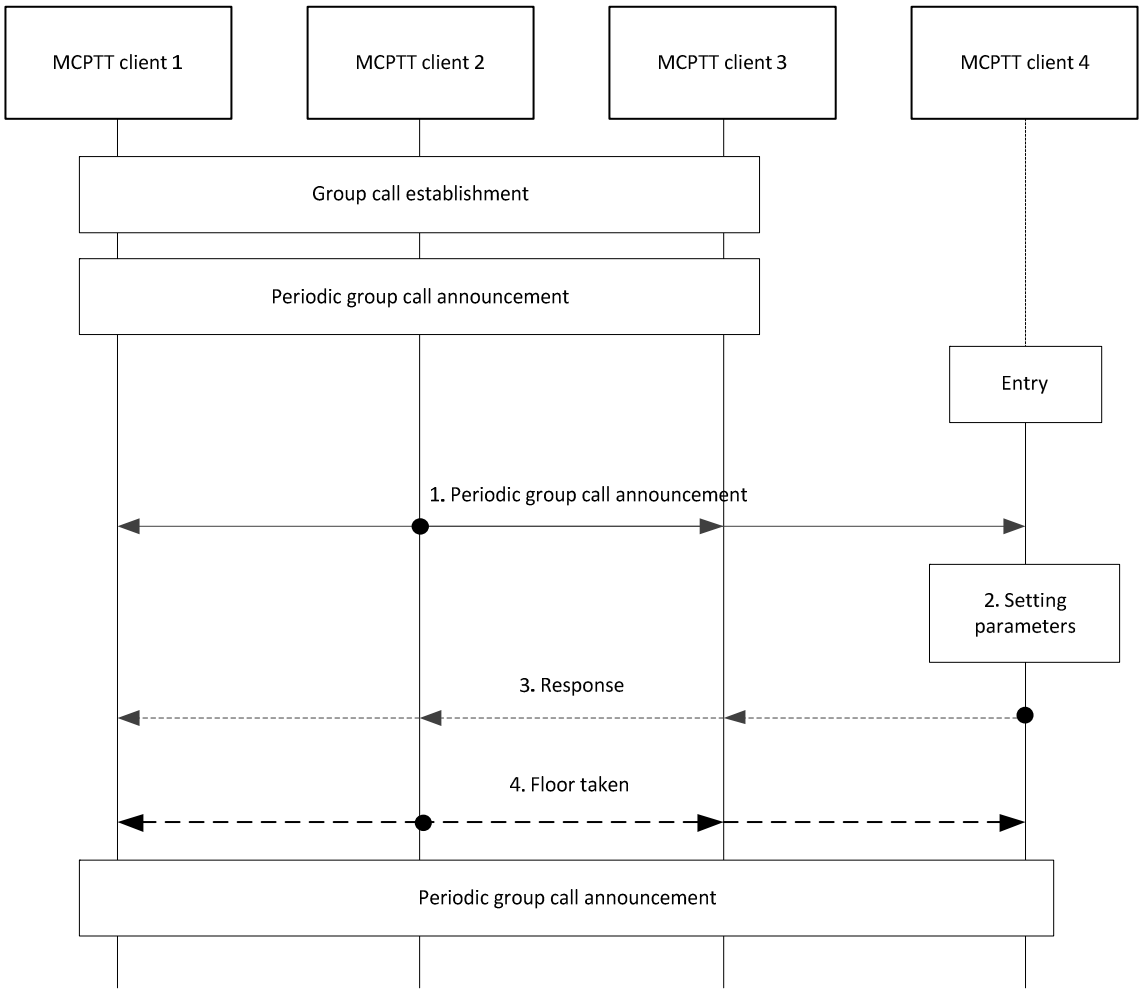

Figure 10.6.3.4-1: Passive join to group call

1. MCPTT client 2 sends the group call announcement message. This message contains the following parameters such as group identity, group call originator identity, media type, media codec, bandwidth, multicast port number for media, port number for floor control protocol, any encryption key for the media encryption if needed, and optionally confirm mode indication.

NOTE 1: The group call announcement includes at least one common set of parameters and values for media transfer. Additional values per parameter will not be prohibited for the better user experience.

2. MCPTT client 4 configures the parameters for media transfer by making use of the received parameters in group call announcement.

3. MCPTT client 4 may send the response message to the group when the periodic group call announcement includes confirm mode indication. This message contains the MCPTT ID.

4. MCPTT client 1, 2, 3 check through the received response message that the MCPTT client 4 joins the group call. The MCPTT client 2, as the floor control arbitrator, may send a floor taken message.

NOTE 2: Due to the movement of the participants (in and out of the radio coverage) during the off-network group call, the group call announcement message including parameters for media delivery is periodically sent.

NOTE 3: The participating MCPTT clients do not need to respond to the periodic group call announcement.

10.6.3.5 Join to ongoing group call when new entry member initiates the call with on-going group call id

Figure 10 6.3.5-1 illustrates the control plane procedures for an MCPTT client to join an on-going MCPTT group call. When entering the coverage of on-going group call, new MCPTT client may send group call setup announcement message with on-going group call id. Upon receiving the group call setup announcement, the MCPTT client as a participant of on-going MCPTT group call sends parameters for media transfer to the newly entered MCPTT client (entrant) to join the on-going MCPTT group call. When receiving the parameters for media transfer of on-going MCPTT group call, the MCPTT client configures the parameters to receive the voice and becomes the participant of the on-going MCPTT group call.

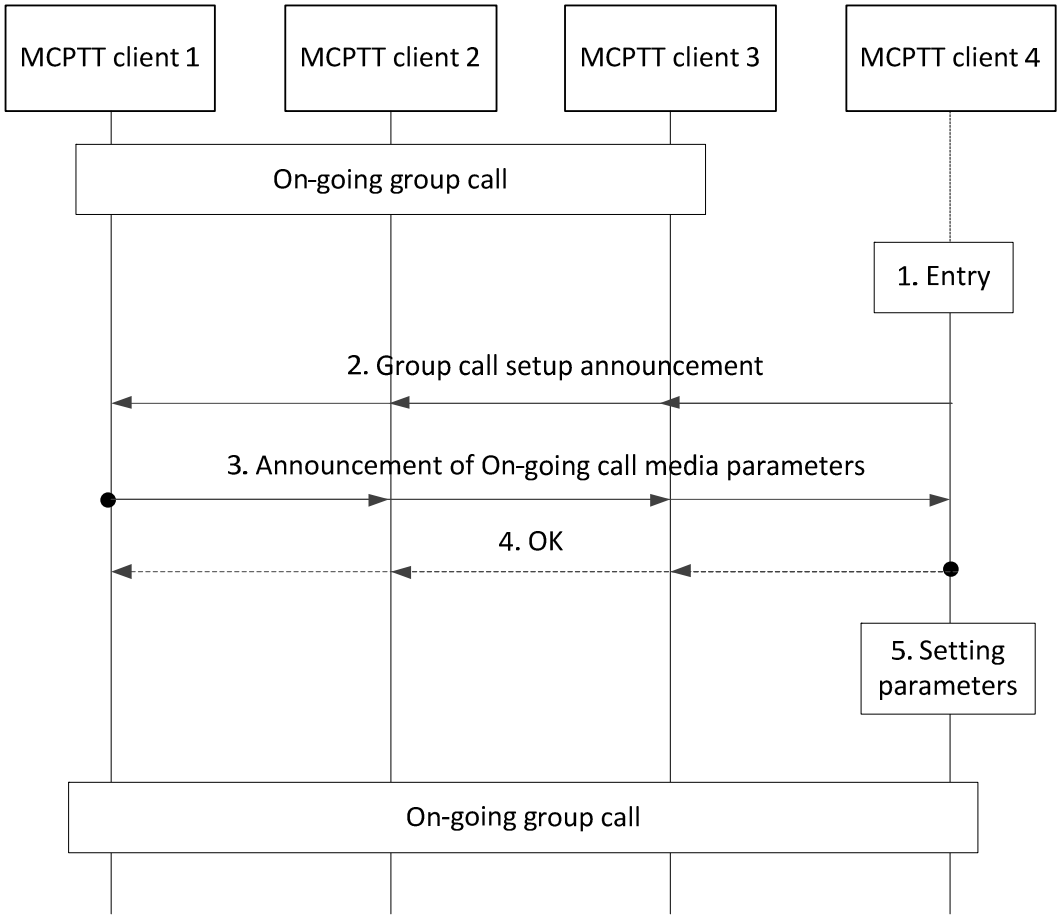

Figure 10.6.3.5-1: Late entry join when receiving MCPTT group call announcement with on-going MCPTT group ID

1. MCPTT client 4 enters the coverage of the on-going MCPTT group call.
2. The new entry of MCPTT client 4 sends group call setup announcement with MCPTT group call id.
3. MCPTT client 1 as a participant of on-going MCPTT group call acknowledges that on-going MCPTT group call exists with MCPTT group call id sent by MCPTT client 4 and sends parameters for media transfer to MCPTT client 4.
4. MCPTT client 4 may send a response message.
5. MCPTT client 4 sets the parameters for media delivery in the on-going MCPTT group call.

MCPTT client 4 joins and becomes participants of the on-going MCPTT group call.

10.6.3.6 Immediate group call announcement to join an ongoing group call

Figure 10.6.3.6-1 illustrates the control plane procedures for an MCPTT client to immediately join an on-going MCPTT group call. Upon the detection of a new entrant, the MCPTT client that is the current talker (floor arbitrator) immediately sends the group call announcement. When receiving the group call announcement message with parameters for media transfer, that MCPTT client configures the parameters to receive the voice and joins the on-going MCPTT group call.

Pre-conditions:

1. There is on-going group call. MCPTT client 1 is the current talker and therefore the floor arbitrator.

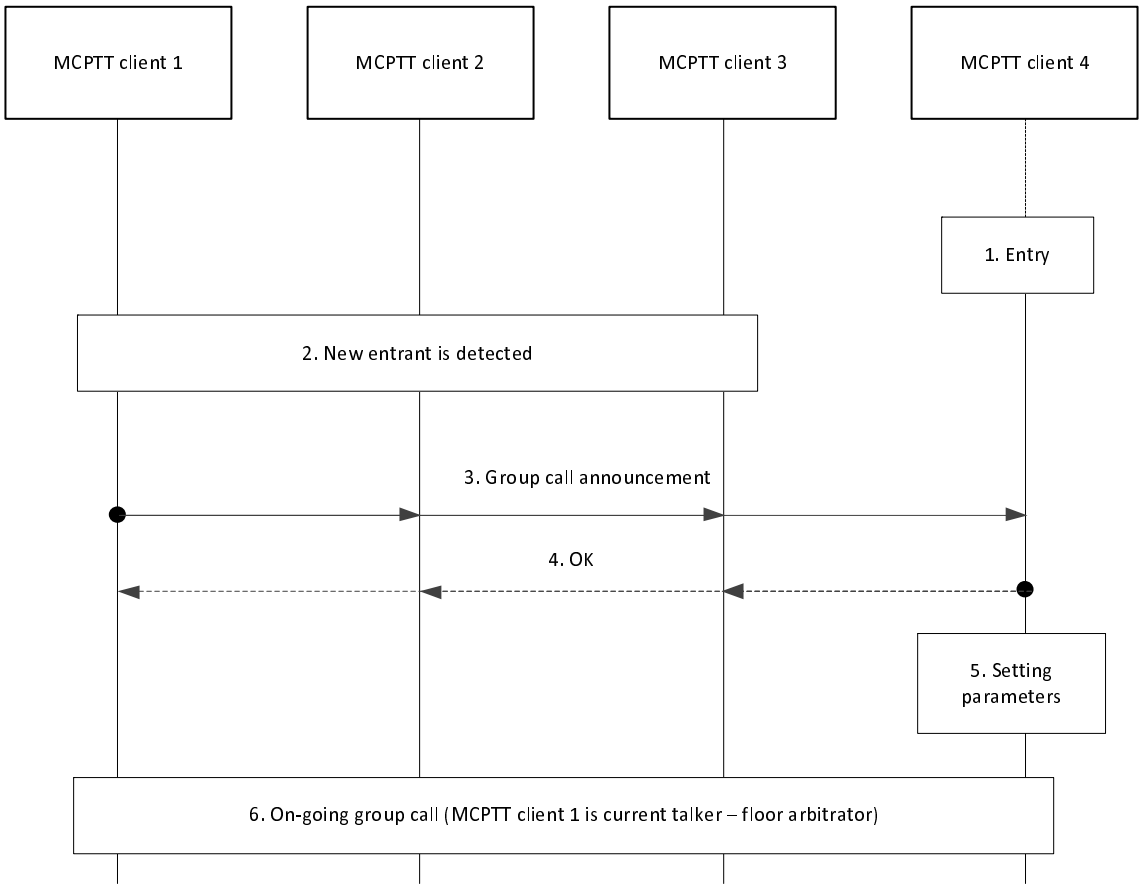

Figure 10.6.3.6-1: Immediate group call announcement to join an ongoing group call

1. MCPTT client 4 enters the coverage of the on-going MCPTT group call.
2. The entry of MCPTT client 4 is detected by the current participants.
3. Since MCPTT client 1 is the current talker (floor arbitrator), MCPTT client 1 immediately sends the group call announcement with the call parameters to the group.
4. MCPTT client 4 may send a response message.
5. MCPTT client 4 sets the parameters for the group call.
6. All participants are now considered part of the on-going group call.

10.6.3.7 Group call release due to inactivity

If the on-going MCPTT group call is inactive for a specific duration, the participating MCPTT clients release the MCPTT group call by themselves.

NOTE: Inactivity time can be set according to the policy of MCPTT service provider.

10.6.3.8 Broadcast group call in off-network

Group call on group-broadcast group and user-broadcast group are handled without distinction in off-network.

Figure 10 6.3.8.1-1 illustrates the control plane procedures for broadcast group call in off-network.

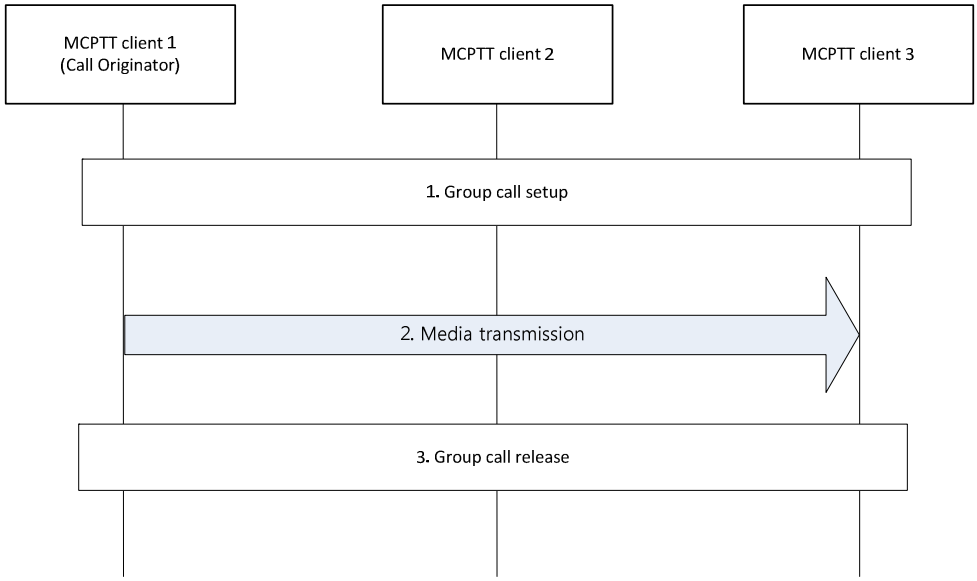

Figure 10.6.3.8.1-1: Broadcast group call in off-network

1. An authorized MCPTT client 1 initiates broadcast group call setup as described in subclause 10.6.3.3. The group call announcement message includes the indication of broadcast group call.
2. The MCPTT client 1 initiating broadcast group call starts to transmit media.

NOTE: Other clients of group member are not allowed to transmit media in broadcast group call.

3. The broadcast group call is released as described in subclause 10.6.3.7.

10.6.3.9 Emergency and imminent peril procedures

10.6.3.9.1 Emergency group call

The off-network emergency group call is a special case of off-network (non-emergency) group call as defined in subclauses 10.6.3.2, 10.6.3.3, 10.6.3.4, 10.6.3.5, 10.6.3.6 and 10.6.3.7. The following are modifications to the aforementioned subclauses to support MCPTT emergency group calls:

- As a pre-condition, the client initiating the emergency call has previously been provisioned with an MCPTT group designated as the MCPTT emergency group. The MCPTT client initiates MCPTT emergency group calls on this group. Alternatively, the MCPTT client could have been provisioned for emergency behaviour on the selected MCPTT group.
- The group call announcement contains an indication that the MCPTT group call is to be an MCPTT emergency call. Group call participants learn of the MCPTT group in-progress emergency condition from the indication.
- The MCPTT client enters the MCPTT emergency state when initiating an MCPTT emergency call. Only the MCPTT user of the MCPTT client can clear the client's local MCPTT emergency state.
- The MCPTT group in-progress emergency state is considered cancelled when the call ends.
- The originating MCPTT user of the in-progress emergency or an authorized user may cancel the in-progress emergency state with an MCPTT emergency group cancel message. The message is sent to the call participants.
- When the MCPTT group is no longer in the in-progress emergency state, every client returns its bearer to the priority it had prior to the in-progress emergency state.
- An MCPTT upgrade to an MCPTT emergency call is used to upgrade an MCPTT group call already in progress. The message is sent to all call participants so that they are aware of the in-progress emergency.
- The bearer is upgraded by all participants for the MCPTT group call already in progress when the MCPTT group call is upgraded to the in-progress emergency state.

- MCPTT group calls on any MCPTT group initiated while the MCPTT user is in MCPTT emergency state will start with a priority bearer.

- An MCPTT emergency group call puts the MCPTT group into the in-progress emergency state. The MCPTT group remains in the in-progress emergency state until the call ends or the in-progress state is cancelled.

NOTE 1: MCPTT group members who are not in the MCPTT emergency state themselves interact with the MCPTT emergency group with elevated bearer priority. These MCPTT group members do not enter the MCPTT emergency state by interacting with the MCPTT group that is in the in-progress emergency state.

10.6.3.9.2 MCPTT imminent peril

The off-network imminent peril group call is a special case of off-network (non-imminent peril) group call as defined in subclauses 10.6.3.2, 10.6.3.3, 10.6.3.4, 10.6.3.5, 10.6.3.6 and 10.6.3.7. The following are modifications to the aforementioned subclauses to support MCPTT imminent peril calls:

- As a pre-condition, the user initiating the imminent peril call has previously an MCPTT group to be used as the MCPTT imminent peril group. The MCPTT client initiates MCPTT imminent peril group calls on this group.

- The group call announcement contains an indication that the MCPTT group call is to be an MCPTT imminent peril call. Group call participants learn of the MCPTT group in-progress imminent peril condition from the indication.

- The MCPTT group in-progress imminent peril state is considered cancelled when the call ends.

- The originating MCPTT user of the in-progress imminent peril or an authorized user may cancel the in-progress imminent peril state with an MCPTT imminent peril group cancel. The message is sent to the call participants.

- When the MCPTT in-progress imminent peril is no longer in the in-progress imminent peril state, every MCPTT client returns its bearer to the priority it had prior to the in-progress imminent peril state.

- An MCPTT upgrade to imminent peril call is used to upgrade an MCPTT group call already in progress. The message is sent to all call participants so that they are aware of the in-progress imminent peril.

- The bearer is upgraded by all participants for the MCPTT group call already in progress when the MCPTT group call is upgraded to in-progress imminent peril state.

- An MCPTT imminent peril call puts the MCPTT group into the in-progress imminent peril state.

10.6.3.9.3 MCPTT emergency alert

10.6.3.9.3.1 MCPTT emergency alert initiation

An MCPTT client initiates an MCPTT emergency alert to the members of an MCPTT group. This procedure will place the MCPTT client in the MCPTT emergency state if the MCPTT client is not already in that state.

Procedures in figure 10.6.3.9.3.1-1 are the signalling control plane procedures for the MCPTT client initiating an MCPTT emergency alert with an MCPTT group i.e., MCPTT users on MCPTT client 1, MCPTT client 2 and MCPTT client 3 belong to the same MCPTT group.

Pre-conditions:

1. The pre-conditions for off-network group calls as described in subclause 10.6.3.3 apply.

2. The initiating MCPTT client 1 has been provisioned with an MCPTT group designated as the MCPTT emergency group.

NOTE 1: Alternatively, MCPTT client 1 could have been provisioned for emergency behaviour on the currently selected group.

3. MCPTT clients 2 and 3 belong to and are ready for off-network communications on the MCPTT group.

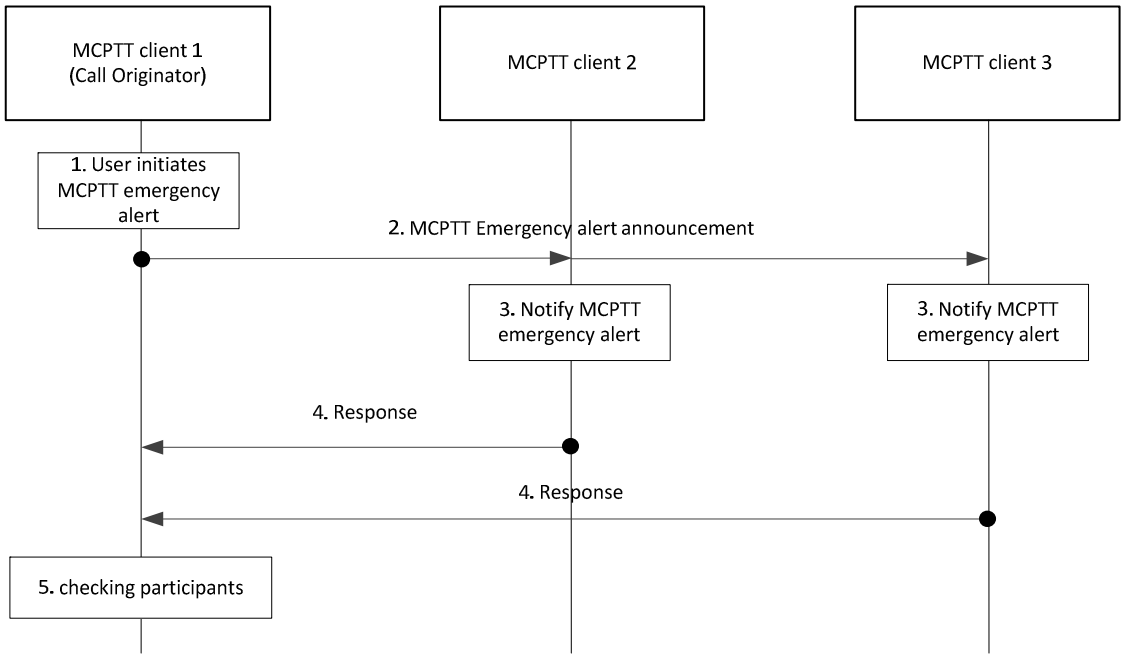

Figure 10.6.3.9.3.1-1: MCPTT emergency alert

1. The user at the MCPTT client 1 initiates an MCPTT emergency alert by sending an MCPTT emergency alert announcement to the other clients. MCPTT client 1 sets its MCPTT emergency state. The MCPTT emergency state is retained by the MCPTT client until explicitly cancelled. Once MCPTT client1 is in the MCPTT emergency state, any calls initiated by MCPTT client 1, group or private, shall be initiated as emergency calls and receive priority treatment. The MCPTT emergency alert announcement is sent periodically so that late joining MCPTT group members are notified.

2. MCPTT client 1 sends an MCPTT emergency alert announcement to the other participants on the MCPTT emergency group.

NOTE 2: Sending the emergency alert without making a request to also start an MCPTT emergency call does not put the group into the in-progress emergency condition.

3. MCPTT users are notified of the MCPTT emergency state of the originating MCPTT user.

4. The receiving MCPTT clients acknowledge the MCPTT emergency alert to the originating MCPTT client.

NOTE 3: Sending the emergency alert without making a request to also start an emergency call does not put the group into the in-progress emergency condition.

NOTE 4: The MCPTT client 1 need not initiate a group call. For example, the MCPTT client can be configured to only allow alerts or the MCPTT user can choose not to make an MCPTT emergency group call.

NOTE 5: MCPTT clients receiving subsequent MCPTT emergency alert announcements that are sent periodically need only respond to the first one that they receive.

5. The originating MCPTT client 1 checks the responses and may inform the MCPTT user of the MCPTT group members whose MCPTTT clients responded.

10.6.3.9.3.2 MCPTT emergency state cancel

An MCPTT client has initiated an MCPTT emergency alert, has entered the MCPTT emergency state and wishes to cancel this state, informing the other MCPTT group members of the cancellation. As part of this process, the MCPTT client may also request the cancellation of the in-progress emergency condition in the group if authorized to do so.

Procedures in figure 10.6.3.9.3.2-1 are the signalling control plane procedures for the MCPTT client cancelling an MCPTT emergency state with an MCPTT group i.e., MCPTT users on MCPTT client 1, MCPTT client 2 and MCPTT client 3 belong to the same MCPTT group.

Pre-conditions:

1. The MCPTT client 1 had previously successfully initiated an MCPTT emergency alert.
2. The MCPTT client 1 is still in the MCPTT emergency state.
3. The initiating MCPTT client 1 and MCPTT clients 2 and 3 are still in off-network contact via the MCPTT group designated provisioned to MCPTT client 1 as the MCPTT emergency group.

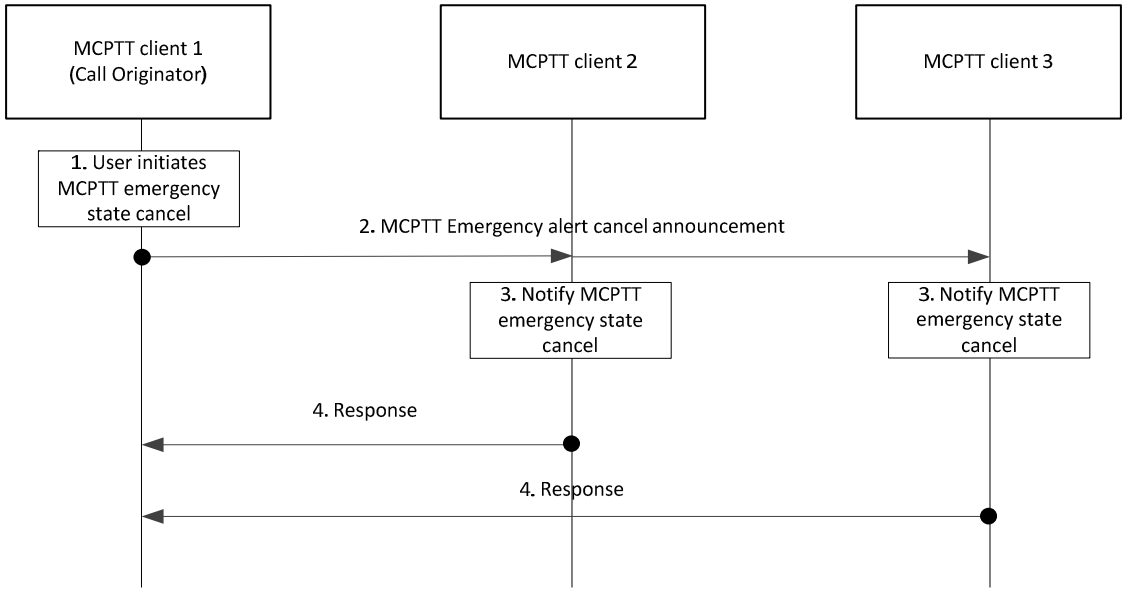

Figure 10.6.3.9.3.2-1 MCPTT emergency state cancel

1. The user at the MCPTT client 1 initiates an MCPTT emergency state cancel.
2. MCPTT client 1 sends an MCPTT emergency state cancel announcement to the MCPTT group to which MCPTT client 1 had previously sent the emergency alert.
3. MCPTT users are notified of the MCPTT emergency cancellation by MCPTT client 1.
4. The receiving MCPTT clients acknowledge the MCPTT emergency state cancel to the originating MCPTT client.

NOTE: MCPTT clients that track the MCPTT emergency alerts of other MCPTT users, e.g. consoles, that fail to receive subsequent periodic MCPTT emergency alert announcements after a configured timeout can consider the alert to be cancelled.

10.7 Private call

10.7.1 General

Private calls are enabled in both on-network and off-network.

Private calls can be setup in two different commencement modes, automatic commencement mode and manual commencement mode.

Private calls in on-network can be with or without floor control. Private calls in off-network are with floor control.

10.7.2 Private call in on-network

10.7.2.1 Information flows for private call in on-network

10.7.2.1.1 MCPTT private call request (originating)

Table 10.7.2.1.1-1 describes the information flow MCPTT private call request from the MCPTT client to the MCPTT server.

Table 10.7.2.1.1-1: MCPTT private call request information elements

Information Element	Status	Description
MCPTT ID	M	The identity of the calling party
MCPTT ID (called party)	M	The identity of the called party
Media parameter information	O	Media parameters of MCPTT client.
Requested commencement mode	O	An indication that is included if the user is requesting a particular commencement mode
Implicit floor request	O	An indication that the user is also requesting the floor.

10.7.2.1.2 MCPTT private call request (MCPTT server – MCPTT server)

Table 10.7.2.1.2-2 describes the information flow MCPTT private call request from the MCPTT server to the MCPTT server.

Table 10.7.2.1.2-2: MCPTT private call request information elements

Information Element	Status	Description
MCPTT ID (originator)	M	The identity of the calling party
MCPTT ID (called party)	M	The identity of the called party
Media parameter information	M	Media parameters of MCPTT client.
Requested commencement mode	O	An indication of the commencement mode to be used.
Implicit floor request	O	An indication that the user is also requesting the floor.

10.7.2.1.3 MCPTT private call response(terminating side)

Table 10.7.2.1.3-1 describes the information flow MCPTT private call response from the MCPTT client to the MCPTT server.

Table 10.7.2.1.3-1: MCPTT private call response information elements

Information Element	Status	Description
MCPTT ID (originator)	M	The identity of the calling party
MCPTT ID (called party)	O	The identity of the called party
Media parameter information	M	Media parameters of MCPTT client.
Requested commencement mode	O	An indication of the commencement mode to be used.

10.7.2.1.4 MCPTT private call response

Table 10.7.2.1.4-2 describes the information flow MCPTT private call response from the MCPTT server to the MCPTT server and the MCPTT server to the MCPTT client.

Table 10.7.2.1.4-2: MCPTT private call response information elements

Information Element	Status	Description
MCPTT ID (originator)	M	The identity of the calling party
MCPTT ID (called party)	O	The identity of the called party
Acceptance confirmation	O	An indication whether the user has positively accepted the call.

10.7.2.1.5 MCPTT emergency private call request

Table 10.7.2.1.5-1 describes the information flow MCPTT emergency private call request from the MCPTT client to the MCPTT server.

Table 10.7.2.1.5-1: MCPTT emergency private call request information elements

Information Element	Status	Description
MCPTT ID	M	The identity of the calling party
MCPTT ID (called party)	M	The identity of the called party
Emergency indicator	M	Indicates that the private call request is an MCPTT emergency call
Alert indicator	M	Indicates whether an emergency alert is to be sent

10.7.2.2 Private call within one MCPTT system

10.7.2.2.1 Private call setup in automatic commencement mode

The procedure focuses on the case where an MCPTT user is initiating an MCPTT private call for communicating with another MCPTT user, with or without floor control enabled, in an automatic commencement mode.

Procedures in figure 10.7.2.2.1-1 are the basic signalling control plane procedures for the MCPTT client initiating establishment of MCPTT private call with the chosen MCPTT user.

Pre-conditions:

1. The calling MCPTT user has selected automatic commencement mode for the call; or
2. The called MCPTT client is set to automatic commencement mode.

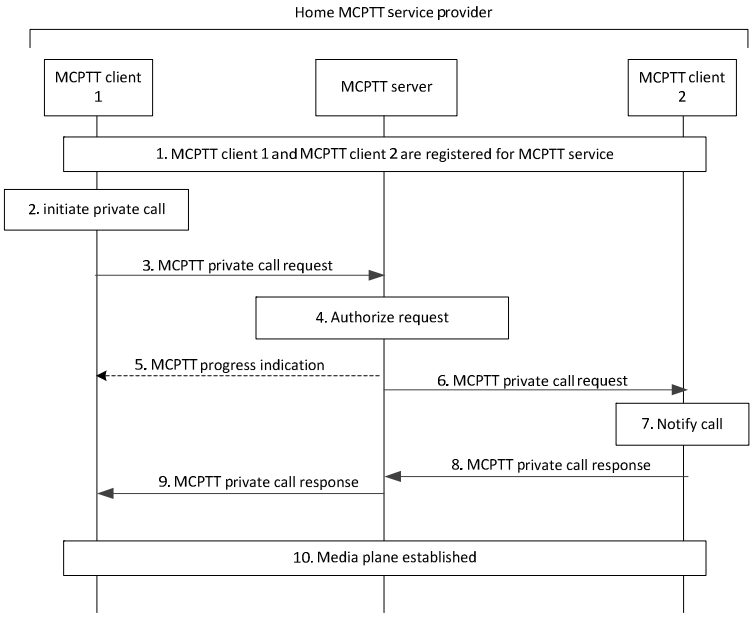

Figure 10.7.2.2.1-1: Private call setup in automatic commencement mode– MCPTT users in the same MCPTT system

1. MCPTT users on MCPTT client 1 and MCPTT client 2 are already registered for receiving MCPTT service, as per procedure in subclause 10.2.

2. User at MCPTT client 1 would like to initiate an MCPTT private call for the chosen MCPTT user. In case of private call with floor control, floor control is to be established.

3. MCPTT client 1 sends an MCPTT private call request towards the MCPTT server (via SIP core) using a service identifier as defined in 3GPP TS 23.228 [5] for MCPTT, for establishing a private call with the chosen MCPTT user. The MCPTT private call request contains the MCPTT id of invited user, an SDP offer containing one or more media types. In case of private call with floor control, the MCPTT private call request also contains an element that indicates that MCPTT client 1 is requesting the floor. The MCPTT client 1 may include a Requested commencement mode that indicates that the call is to be established in automatic commencement mode if automatic commencement mode is requested by the initiating user.

4. MCPTT server checks whether the MCPTT user at MCPTT client 1 is authorized to initiate the private call, and that MCPTT user at MCPTT client 2 is authorized to receive the private call. If the MCPTT private call request requested automatic commencement mode then the MCPTT server also checks whether the MCPTT user at MCPTT client 1 is authorized to initiate a private call in automatic commencement mode.

5. MCPTT server may provide a progress indication to MCPTT client 1 to indicate progress in the call setup process.

NOTE: Step 5 can occur at any time following step 4, and prior to step 9.

6. If authorized, MCPTT server includes information that it communicates using MCPTT service, offers the same media types or a subset of the media types contained in the initial received request, includes the requested automatic commencement mode indication based on a requested automatic commencement mode by the calling user or based upon the setting of the called MCPTT client and sends the corresponding MCPTT private call request towards the MCPTT client 2, including the MCPTT ID of the calling MCPTT user 1. If the called MCPTT user has registered to the MCPTT service with multiple MCPTT UEs and has designated the MCPTT UE for receiving the private calls, then the incoming MCPTT private call request is delivered only to the designated MCPTT UE.

7. The receiving MCPTT client 2 notifies the user about the incoming private call.

8. The receiving MCPTT client 2 accepts the private call automatically, and an MCPTT private call response is sent to the MCPTT server (via SIP core).

9. Upon receiving the MCPTT private call response from MCPTT client 2 accepting the private call request, the MCPTT server informs the MCPTT client 1 about successful call establishment.

10. MCPTT client 1 and MCPTT client 2 have successfully established media plane for communication and either user can transmit media. In case of successful call establishment for private call with floor control request from MCPTT client 1, floor participant at MCPTT client 1 is granted floor by the floor control server, giving it permission to transmit. At the same time floor participant at MCPTT client 2 is informed by the floor control server that floor is taken.

10.7.2.2.2 Private call setup in manual commencement mode

10.7.2.2.2.1 Description

Figure 10.7.2.2.2.2-1 describes the basic procedure for the MCPTT client initiating an MCPTT private call that uses manual commencement mode. The flow may use a floor request in the MCPTT private call request indicating that the originator will be given the floor when the call starts and eliminates the need for a separate initial floor request message during media plane establishment. Alternatively the call initiation may be sent without the floor request, which allows the called party to request the floor first.

10.7.2.2.2.2 Procedure

Both clients are served by the primary MCPTT service provider in figure 10.7.2.2.2.2-1.

Pre-conditions:

1. The calling MCPTT user has selected manual commencement mode or has not specified a commencement mode for the call; and

2. The called MCPTT client is set to manual commencement mode.

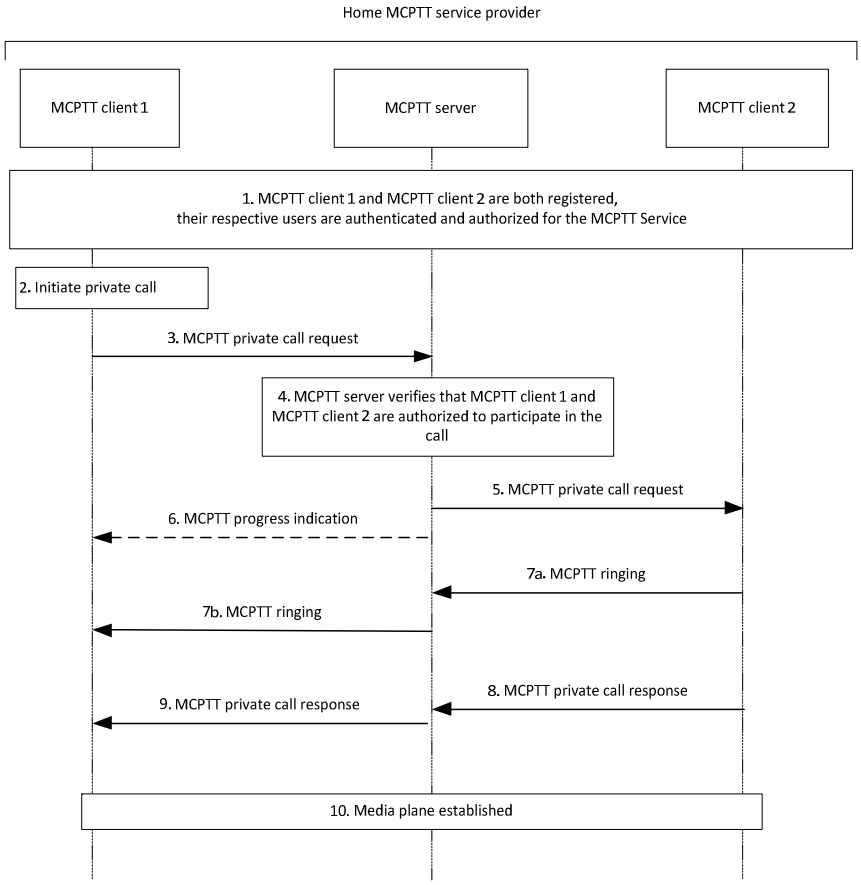

Figure 10.7.2.2.2.2-1: MCPTT private call in manual commencement mode– MCPTT users in the same MCPTT system

1. MCPTT client 1 and MCPTT client 2 are both registered and their respective users, MCPTT user 1 and MCPTT user 2, are authenticated and authorized to use the MCPTT service, as per procedure in subclause 10.2.

2. MCPTT user at MCPTT client 1 would like to initiate an MCPTT private call for the selected MCPTT user. In case of private call with floor control, floor control is to be established. In the case of private call without floor control, both users will have the ability to transmit without floor arbitration.

3. MCPTT client 1 sends an MCPTT private call request addressed to the MCPTT ID of MCPTT user 2 using an MCPTT service identifier as defined in 3GPP TS 23.228 [5] (possible for the SIP core to route the request to the MCPTT server). The MCPTT private call request contains the MCPTT ID of invited user and an SDP offer containing one or more media types. The MCPTT private call request may also contain a data element that indicates that MCPTT client 1 is requesting the floor, in the case of private call with floor control. The MCPTT client 1 may include a requested commencement mode that indicates that the call is to be established in manual commencement mode if manual commencement mode is requested by the initiating user.

4. The MCPTT server confirms that both MCPTT users are authorized for the private call. The MCPTT server checks the commencement mode setting of the called MCPTT client and also checks whether the MCPTT user at MCPTT client 1 is authorized to initiate a call in manual commencement mode.

5. The MCPTT server includes information that it communicates using MCPTT service, offers the same media types or a subset of the media types contained in the initial received request and sends an MCPTT private call request for the call to MCPTT client 2, including the MCPTT ID of the calling MCPTT user 1. If the called MCPTT user has registered to the MCPTT service with multiple MCPTT UEs and has designated the MCPTT UE for receiving the private calls, then the incoming MCPTT private call request is delivered only to the designated MCPTT UE.

6. MCPTT server may provide a progress indication to MCPTT client 1 to indicate progress in the call setup process.

NOTE: Step 6 can occur at any time following step 4, and prior to step 7b.

7a. The MCPTT user is alerted. MCPTT client 2 sends an MCPTT ringing to the MCPTT server.

7b. The MCPTT server sends an MCPTT ringing to MCPTT client 1, indicating that MCPTT client 2 is being alerted.

8. MCPTT user 2 has accepted the call using manual commencement mode (i.e., has taken some action to accept via the user interface) which causes MCPTT client 2 to send an MCPTT private call response to the MCPTT server. If MCPTT user 2 has not accepted the incoming call, the MCPTT client 2 sends a call failure response to the MCPTT server without adding reason for call failure.

9. The MCPTT server sends an MCPTT private call response to MCPTT client 1 indicating that MCPTT user 2 has accepted the call, including the accepted media parameters.

10. The media plane for communication is established. Either user can transmit media individually when using floor control. In the case of successful call establishment for private call with floor request from MCPTT client 1, the floor participant associated with MCPTT client 1 is granted the floor initially. At the same time the floor participant associated with MCPTT client 2 is informed that the floor is taken. The meaning of the floor request (give floor initially to originator [client 1], or give floor initially to target [client 2]) may be configurable. In the case of private call without floor control both users are allowed to transmit simultaneously.

10.7.2.2.3 Private call release

10.7.2.2.3.1 Client initiated

The procedure focuses on the case where an MCPTT client is requesting to release an ongoing MCPTT private call (with or without floor control) and the call established in either of the two commencement modes (manual or automatic).

Procedures in figure 10.7.2.2.3.1-1 are the basic signalling control plane procedures for the MCPTT client initiating the release of an ongoing MCPTT private call.

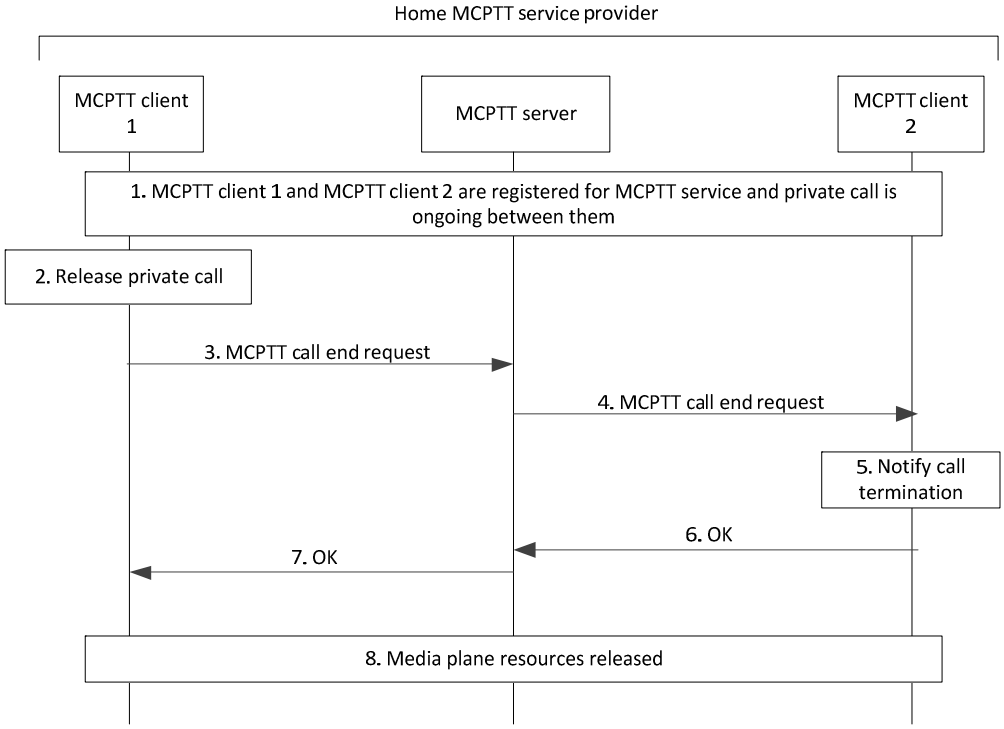

Figure 10.7.2.2.3.1-1: Private call release – client initiated

1. It is assumed that MCPTT users on MCPTT client 1 and MCPTT client 2 are already registered for receiving MCPTT service and are involved in private call with or without floor control established either in manual or automatic commencement mode, as described in subclause 10.7.2.2.1 and subclause 10.7.2.2.2.
2. User at MCPTT client 1 would like to release an ongoing MCPTT private call with MCPTT client 2.
3. MCPTT client 1 sends an MCPTT call end request towards the MCPTT server (via SIP core), for tearing down the private call with the other client.
4. MCPTT server sends the corresponding MCPTT call end request towards the MCPTT client specified in the original MCPTT call end request.
5. MCPTT user is notified about the release of the private call.
6. The receiving MCPTT client 2 acknowledges the MCPTT call end request.
7. After receiving the MCPTT call end request acknowledgement from MCPTT client 2, the MCPTT server generates an acknowledgement for the MCPTT client 1's MCPTT call end request.
8. MCPTT clients release all the media plane resources used for the private call. Further, if the private call was established with floor control, floor control resources are released and MCPTT clients cannot make further requests for floor control or send media.

10.7.2.2.3.2 Server initiated

The procedure focuses on the case where an MCPTT server is terminating an ongoing MCPTT private call (with or without floor control) and the call established in either of the two commencement modes (manual or automatic), upon conditions to terminate call e.g., MCPTT administrator configured maximum duration for MCPTT private calls has expired or timed out due to MCPTT private call without transmission/reception.

Procedures in figure 10.7.2.2.3.2-1 are the basic signalling control plane procedures for the MCPTT server initiating termination of an ongoing MCPTT private call.

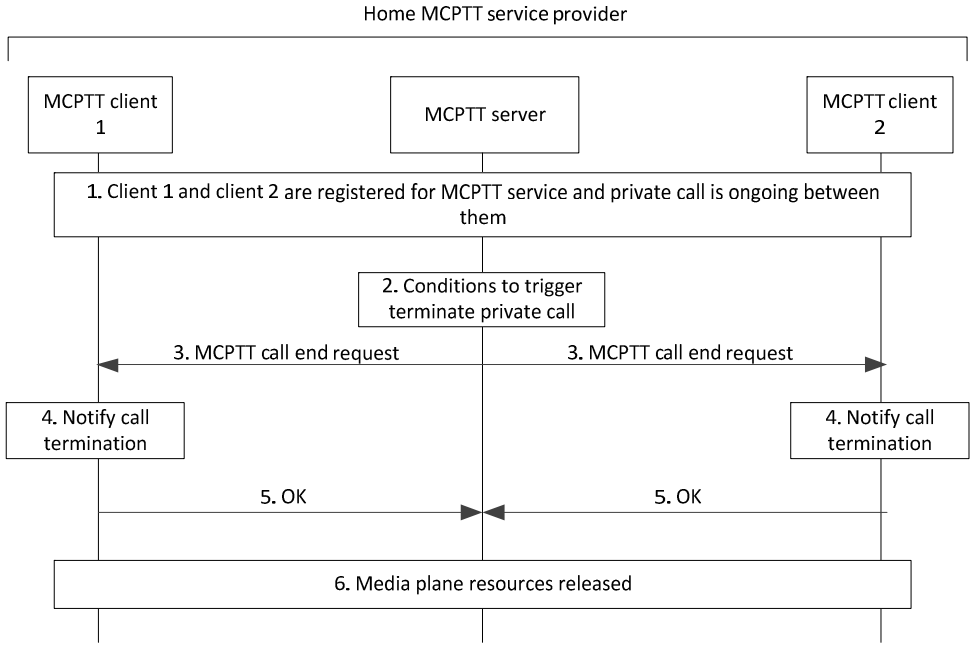

Figure 10.7.2.2.3.2-1: End private call – server initiated

1. It is assumed that MCPTT users on MCPTT client 1 and MCPTT client 2 are already registered for receiving MCPTT service and are involved in private call with or without floor control established either in manual or automatic commencement mode.

2. Upon conditions to terminate call e.g., MCPTT administrator configured maximum duration for MCPTT private calls has expired or timed out due to MCPTT private call without transmission/reception, the MCPTT server decides to initiate termination of an ongoing MCPTT private call between MCPTT client 1 and MCPTT client 2.
3. MCPTT server sends an MCPTT call end request towards the MCPTT clients 1 and 2 (via SIP core), for tearing down the private call between them.
4. MCPTT users at client 1 and client 2 are notified about the termination of the private call.
5. The MCPTT call end request receiving MCPTT clients 1 and 2 acknowledge the request with OK.
6. MCPTT clients release all the media plane resources used for the private call. Further, if the private call was established with floor control, floor control resources are released and MCPTT clients cannot make further requests for floor control or send media.

10.7.2.3 Private call within several MCPTT systems

10.7.2.3.1 Private call setup in automatic commencement mode – MCPTT users in multiple MCPTT systems

The procedure focuses on the case where an MCPTT user is initiating an MCPTT private call (automatic commencement mode) for communicating with MCPTT user in another MCPTT system with or without floor control enabled.

Procedures in figure 10.7.2.3.1-1 are the procedures for the MCPTT client initiating establishment of MCPTT private call with the chosen MCPTT user.

Pre-conditions:

1. The calling MCPTT user has selected automatic commencement mode for the call; or
2. The called MCPTT client is set to automatic commencement mode.

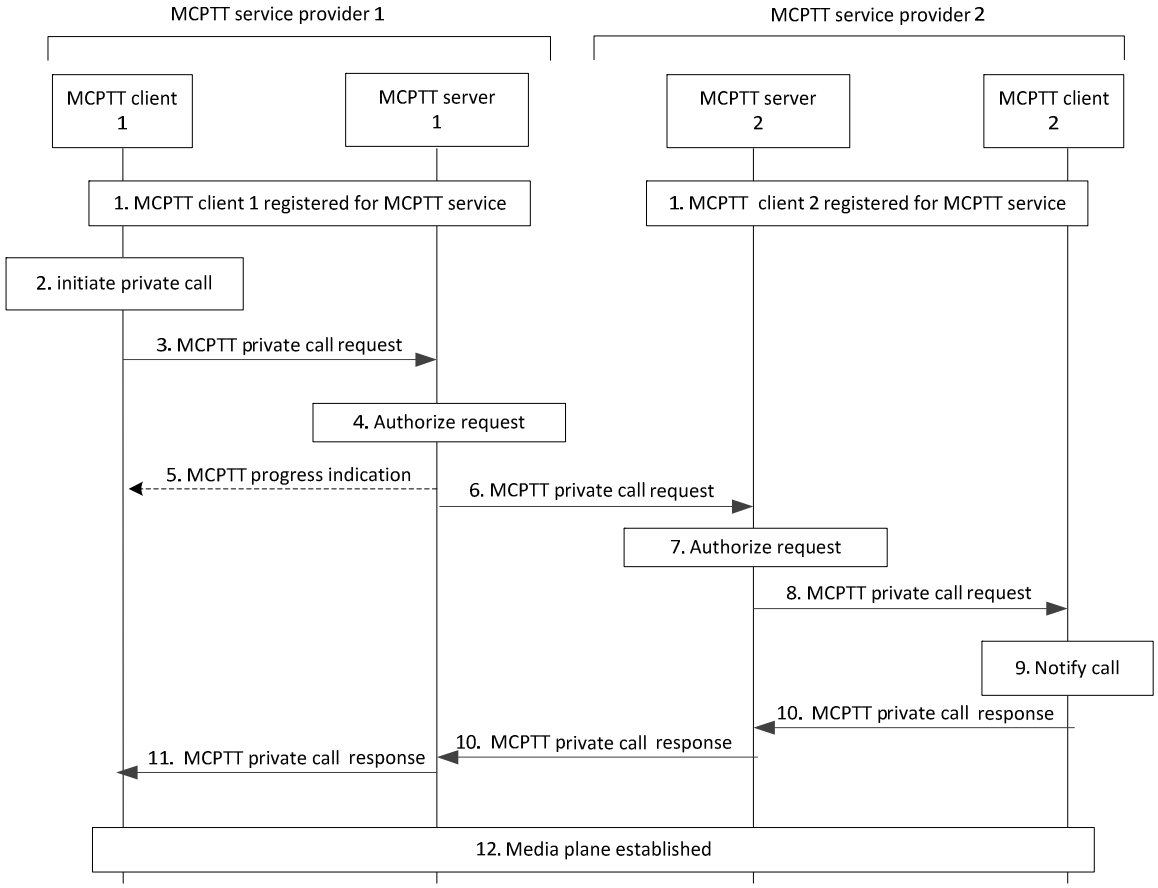

Figure 10.7.2.3.1-1: Private call setup in automatic commencement mode – users in multiple MCPTT systems

1. It is assumed that MCPTT users on MCPTT client 1 and MCPTT client 2 are already registered for receiving MCPTT service to their respective MCPTT service provider, as per procedure in subclause 10.2.

2. MCPTT user at MCPTT client 1 would like to initiate an MCPTT private call for the chosen MCPTT user. In case of private call with floor control, floor control is to be established.

3. MCPTT client 1 sends an MCPTT private call request towards the home MCPTT server 1 (via SIP core) using a service identifier as defined in 3GPP TS 23.228 [5] for MCPTT, for establishing private call with the MCPTT client 2 registered at MCPTT service provider 2. The MCPTT private call request contains the MCPTT id of invited user and an SDP offer containing one or more media types. In case of private call with the floor control, the MCPTT private call request also contains an element that indicates that MCPTT client 1 is requesting the floor. The MCPTT client 1 may include a requested commencement mode that indicates that the call is to be established in automatic commencement mode if automatic commencement mode is requested by the initiating user.

4. MCPTT server 1 checks whether the MCPTT user at MCPTT client 1 is authorized to initiate the private call. If the MCPTT private call request requested automatic commencement mode then the MCPTT server 1 also checks whether the MCPTT user at MCPTT client 1 is authorized to initiate a call in automatic commencement mode.

5. MCPTT server 1 may provide a progress indication to MCPTT client 1 to indicate progress in the call setup process.

NOTE: Step 5 can occur at any time following step 4, and prior to step 11.

6. If authorized, MCPTT server 1 includes information that it communicates using MCPTT service, offers the same media types or a subset of the media types contained in the initial received request, includes an automatic commencement mode indication if automatic commencement mode was requested by and authorised for the

calling user and sends the corresponding MCPTT private call request towards the MCPTT system (via SIP core) of the MCPTT client specified in the original MCPTT private call request (MCPTT client 2) i.e., MCPTT server 2.

7. MCPTT server 2 checks whether the MCPTT user at MCPTT client 2 is authorized to receive a private call.

8. MCPTT server 2 includes information that it communicates using MCPTT service, offers the same media types or a subset of the media types contained in the initial received request, includes a requested automatic commencement mode indication based on a requested automatic commencement mode by the calling user or based upon the setting of the called MCPTT client and sends the received MCPTT private call request towards the MCPTT client specified in the received MCPTT private call request (i.e., MCPTT client 2). If the called MCPTT user has registered to the MCPTT service with multiple MCPTT UEs and has designated the MCPTT UE for receiving the private calls, then the incoming MCPTT private call request is delivered only to the designated MCPTT UE.

9. The receiving MCPTT client 2 notifies the user about the incoming private call.

10. The receiving MCPTT client 2 accepts the private call automatically, and an acknowledgement is sent to the MCPTT server 1 (via SIP core and MCPTT server 2).

11. Upon receiving the MCPTT private call response from MCPTT client 2 accepting the private call request, MCPTT client 1 is informed about successful call establishment.

12. MCPTT client 1 and MCPTT client 2 have successfully established media plane for communication and either user can transmit media. In case of successful call establishment for private call with implicit floor control request from MCPTT client 1, floor participant at MCPTT client 1 is granted floor by the floor control server at MCPTT service provider 1, giving it permission to transmit. At the same time floor participant at MCPTT client 2 is informed by the floor control server at MCPTT service provider 1 that the floor is taken.

10.7.2.3.2 Private call setup in manual commencement mode – MCPTT users in multiple MCPTT systems

The procedure focuses on the case where an MCPTT user is initiating an MCPTT private call (manual commencement mode) for communicating with MCPTT user in another MCPTT system with or without floor control enabled.

Procedures in figure 10.7.2.3.2-1 are the procedures for the MCPTT client initiating establishment of MCPTT private call with the selected MCPTT user.

Pre-conditions:

1. The calling MCPTT user has selected manual commencement mode or has not specified a commencement mode for the call; and

2. The called MCPTT client is set to manual commencement mode.

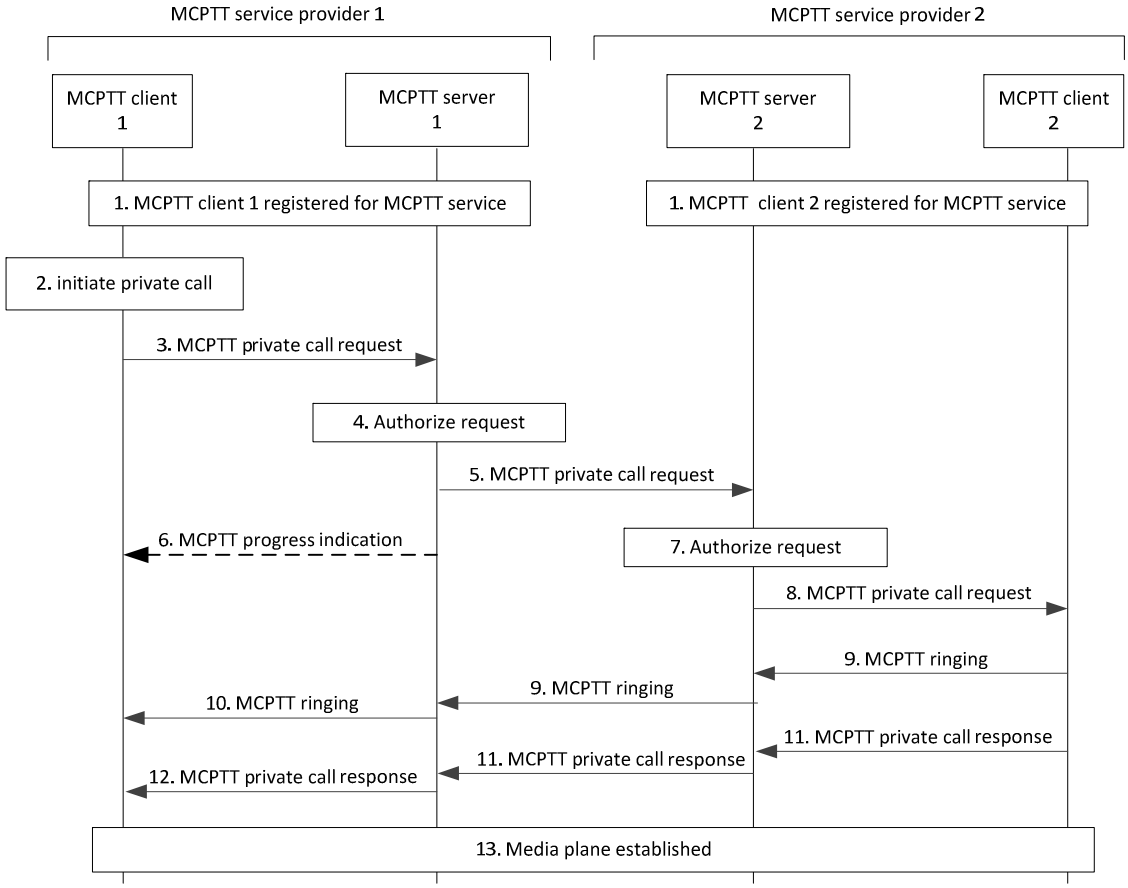

Figure 10.7.2.3.2-1: Private call setup in manual commencement mode – users in multiple MCPTT systems

1. It is assumed that MCPTT users on MCPTT client 1 and MCPTT client 2 are already registered for receiving MCPTT service to their respective MCPTT service provider, as per procedure in subclause 10.2.

2. MCPTT user at MCPTT client 1 would like to initiate an MCPTT private call for the selected MCPTT user. In case of private call with floor control, floor control is to be established.

3. MCPTT client 1 sends an MCPTT private call request towards the home MCPTT server 1 (via SIP core), for establishing private call with the MCPTT client 2 registered at MCPTT service provider 2. In case of private call with the floor control, the MCPTT private call request contains an element that indicates that MCPTT client 1 is requesting the floor. The MCPTT client 1 may include a requested commencement mode that indicates that the call is to be established in manual commencement mode if manual commencement mode is requested by the initiating user.

4. MCPTT server 1 checks whether the MCPTT user at MCPTT client 1 is authorized to initiate the private call. The MCPTT server 1 also checks whether the MCPTT user at MCPTT client 1 is authorized to initiate a call in manual commencement mode.

5. If authorized, MCPTT server 1 sends the corresponding MCPTT private call request towards the MCPTT system (via SIP core) of the MCPTT client specified in the original MCPTT private call request (MCPTT client 2) i.e., MCPTT server 2.

6. MCPTT server may provide a progress indication to MCPTT client 1 to indicate progress in the call setup process.

NOTE: Step 6 can occur at any time following step 4, and prior to step 10.

7. The MCPTT server 2 checks whether the MCPTT user at MCPTT client 2 is authorized to receive a private call and also checks the commencement mode setting of MCPTT client 2.

8. The MCPTT server 2 offers the same media types or a subset of the media types contained in the initial received request and sends an MCPTT private call request towards the MCPTT client specified in the received MCPTT private call request (i.e., MCPTT client 2). If the called MCPTT user has registered to the MCPTT service with multiple MCPTT UEs and has designated the MCPTT UE for receiving the private calls, then the incoming MCPTT private call request is delivered only to the designated MCPTT UE.

9. The MCPTT user is alerted. MCPTT client 2 sends an MCPTT ringing to the MCPTT server 1 (via server 2).

10. The MCPTT server 1 sends an MCPTT ringing to MCPTT client 1, indicating that MCPTT client 2 is being alerted.

11. MCPTT user 2 has accepted the call using manual commencement mode (i.e. has taken some action to accept via the user interface) which causes MCPTT client 2 to send an MCPTT private call response to the MCPTT server 1 (via SIP core and MCPTT server 2)

12. Upon receiving the MCPTT private call response from MCPTT client 2 accepting the private call request, MCPTT client 1 is informed about successful call establishment.

13. MCPTT client 1 and client 2 have successfully established media plane for communication and either user can transmit media. In case of successful call establishment for private call with implicit floor control request from MCPTT client 1, floor participant at MCPTT client 1 is granted the floor by the floor control server at MCPTT service provider 1, giving it permission to transmit. At the same time floor participant at MCPTT client 2 is informed by the floor control server at MCPTT service provider 1 that the floor is taken.

10.7.2.3.3 Private call release – MCPTT users in multiple MCPTT systems

The procedure in this subclause is for the case where an MCPTT client is requesting to release an ongoing MCPTT private call (with or without floor control) established in either of the two commencement modes (manual or automatic), and the MCPTT users are in multiple MCPTT systems.

Procedures are similar to those described for private call release when MCPTT users are in single MCPTT system as in subclause 10.7.2.2.3.1, with the addition that the MCPTT call end request and the corresponding acknowledgement are routed through the MCPTT server in partner MCPTT system.

10.7.2.4 MCPTT emergency private call

10.7.2.4.1 MCPTT emergency private call commencement

This procedure focuses on the case where an authorized MCPTT user is initiating an MCPTT emergency private call with unicast signalling for communicating with another MCPTT user. An MCPTT client in the MCPTT emergency state gains elevated access privilege for all of the MCPTT user's mission critical applications.

Procedures in figure 10.7.2.4.1-1 are the signalling control plane procedures for the MCPTT client initiating establishment of an MCPTT emergency private call.

Pre-conditions:

1. Both members of the MCPTT private call belong to the same MCPTT system.

2. The initiating MCPTT client 1 has been configured to send an MCPTT emergency alert prior to initiating an MCPTT emergency private call.

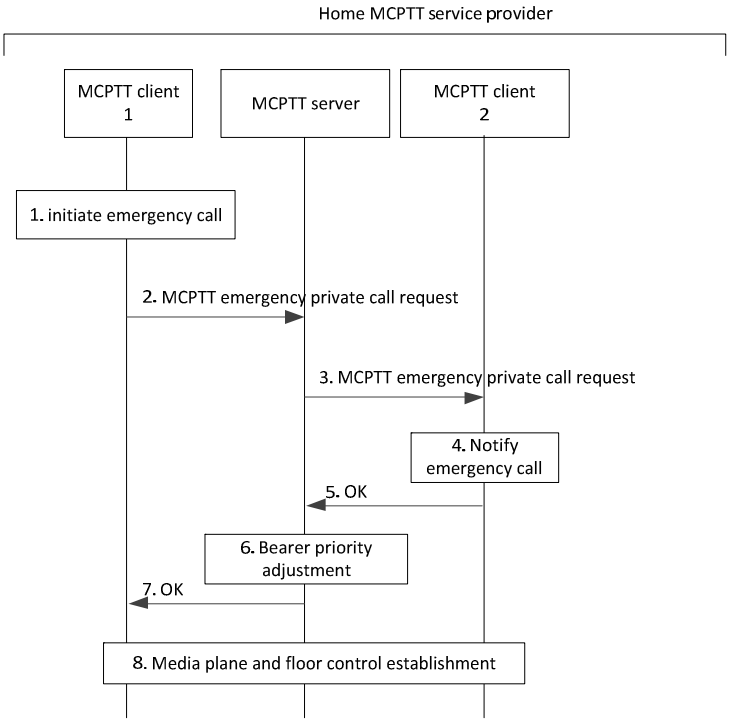

Figure 10.7.2.4.1-1 MCPTT emergency private call

1. The user at the MCPTT client 1 initiates an MCPTT emergency private call. MCPTT client 1 sets its MCPTT emergency state. The MCPTT emergency state is retained until explicitly cancelled.

2. MCPTT client 1 sends an MCPTT emergency private call request towards the MCPTT server. The request contains an indication of the MCPTT emergency. The MCPTT server records the identity of the MCPTT user that initiated the MCPTT emergency private call until the MCPTT emergency is cancelled. If the MCPTT client is configured to send an MCPTT emergency alert when initiating an MCPTT emergency private call, the request also contains an indication that an MCPTT emergency alert is to be initiated.

3. MCPTT server sends the MCPTT emergency private call request towards the target MCPTT client. The request contains an indication of the in-progress emergency. The request contains an indication of an MCPTT emergency alert if the request from the originator indicated MCPTT emergency alert.

4. The MCPTT user on MCPTT client 2 is notified of the incoming MCPTT emergency private call.

5. The receiving MCPTT client acknowledges the MCPTT emergency private call request to the MCPTT server.

6. The MCPTT server adjusts the priority of the underlying bearer.

7. The MCPTT server informs MCPTT client 1 about the successful MCPTT emergency private call establishment.

8. MCPTT client 1 and MCPTT client 2 establish the media plane for communication. The MCPTT client 1 can override MCPTT client 2 unless MCPTT client 2 is also in the MCPTT emergency state.

NOTE 1: The priority for the MCPTT emergency private call is retained until cancelled according to system policy (e.g. timeout or call end) or cancelled by an authorized MCPTT user.

NOTE 2: The initiating MCPTT user's MCPTT emergency state is retained by the system until cancelled as in subclause 10.6.2.6.1.3. The initiating MCPTT user's MCPTT emergency state is also retained locally by the MCPTT client until explicitly cancelled by the MCPTT user.

10.7.2.4.2 MCPTT private call emergency upgrade

This procedure focuses on the case where an authorized MCPTT user is upgrading a private call to an MCPTT emergency private call while the private call is already in progress.

Procedures in figure 10.7.2.4.2-1 are the signalling procedures for the MCPTT client upgrading a private call to an MCPTT emergency private call.

Pre-conditions:

1. Both members of the private call belong to the same MCPTT system.
2. A private call is already in progress.

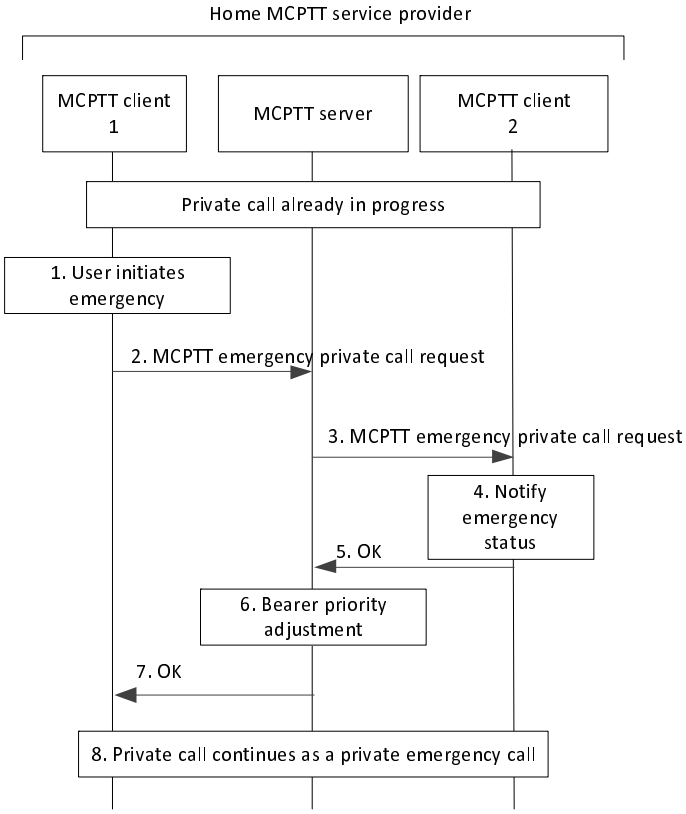

Figure 10.7.2.4.2-1: MCPTT private call upgrade

1. The MCPTT user at MCPTT client 1 initiates an emergency. MCPTT client 1 sets its MCPTT emergency state. The MCPTT emergency state is retained until explicitly cancelled.
2. MCPTT client 1 requests the MCPTT server to upgrade the private call to in-progress emergency by sending an MCPTT emergency request. If configured to send an MCPTT alert when initiating an MCPTT emergency upgrade, the request also contains an indication that an MCPTT alert is to be initiated. The request may contain an indication of an implicit floor request.
3. MCPTT server sends the MCPTT emergency request towards the MCPTT client of the other participant.
4. The MCPTT user is notified of the in-progress emergency of the MCPTT emergency private call.
5. The receiving MCPTT client acknowledges the MCPTT emergency request to the MCPTT server.
6. The MCPTT server adjusts the priority of the underlying bearer for both participants in the private call. The priority is retained until the call ends.
7. The MCPTT server confirms the upgrade request to MCPTT client 1. If the MCPTT emergency request contained an implicit floor request, the OK message contains the result of the implicit floor request.

8. MCPTT client 1 and MCPTT client 2 continue with the private call, which has been transformed into an MCPTT emergency private call. The MCPTT client 1 can override MCPTT client 2 unless MCPTT client 2 is also in the MCPTT emergency state.

10.7.3 Private call in off-network

10.7.3.1 Information flows for private call in off-network

10.7.3.1.1 Call setup request

Table 10.7.3.1.1-1 describes the information flow call setup request from one MCPTT client to another MCPTT client.

Table 10.7.3.1.1-1: call setup request

Information element	Status	Description
MCPTT ID of the caller	M	The identity of the calling party
MCPTT ID of the callee	M	The identity of the called party
Use floor control indication	M	This element indicates whether floor control will be used for the private call. When set to YES floor control will be used.
SDP offer for private call	M	SDP with media information offered by (to) client

10.7.3.1.2 Call setup response

Table 10.7.3.1.2-1 describes the information flow call setup response from one MCPTT client to another MCPTT client.

Table 10.7.3.1.2-1: call setup response

Information element	Status	Description
MCPTT ID of the caller	M	The identity of the calling party
MCPTT ID of the callee	M	The identity of the called party
Use floor control indication	M	This element indicates whether floor control will be used for the private call. When set to YES floor control will be used.
SDP answer for private call	M	SDP with media information offered by (to) client

10.7.3.1.3 Call release request

Table 10.7.3.1.3-1 describes the information flow call release request from one MCPTT client to another MCPTT client.

Table 10.7.3.1.3-1: call release request

Information element	Status	Description
MCPTT ID of the caller	M	The identity of the calling party
MCPTT ID of the callee	M	The identity of the called party
MCPTT private call release reason	O	This element indicates that reason for the private call release. e.g., Originating client requested, target client requested.

10.7.3.1.4 Call release response

Table 10.7.3.1.4-1 describes the information flow call release response from one MCPTT client to another MCPTT client.

Table 10.7.3.1.4-1: call release response

Information element	Status	Description
MCPTT ID of the caller	M	The identity of the calling party
MCPTT ID of the callee	M	The identity of the called party
MCPTT private call release reason	O	This element indicates that reason for the private call release. e.g., Originating client requested, target client requested, server requested.

10.7.3.2 Use of ProSe capability for private call

When an MCPTT user using a ProSe-enabled UE wants to communicate with a specific MCPTT user using a ProSe-enabled UE by a ProSe mechanism, the MCPTT client shall first acquire the IP address and layer-2 ID of the MCPTT UE associated with the target MCPTT user.

To achieve that, the MCPTT client requests the ProSe layer to provide the layer-2 ID and IP address for the target MCPTT UE by providing User Info Id (as defined in specification 3GPP TS 23.303 [8]) of the target MCPTT user. This may trigger the ProSe layer procedure (e.g. discovery). The User Info Id of the target MCPTT user is used by the ProSe layer as the target info (as defined in specification 3GPP TS 23.303 [8]).

The ProSe capability will then provide the layer-2 ID and IP address related to the target MCPTT user's MCPTT ID to the MCPTT client.

10.7.3.3 Private call setup in automatic commencement mode

The procedure focuses on the case where an MCPTT user is initiating an MCPTT private call for communicating with another MCPTT user when off-network using an automatic commencement mode.

Procedures in figure 10.7.3.3-1 are the basic signalling procedures for the MCPTT client initiating establishment of an off-network MCPTT private call with the chosen MCPTT user.

Pre-conditions:

1. MCPTT user profile used for off-network operation mode is pre-provisioned in the MCPTT UEs.

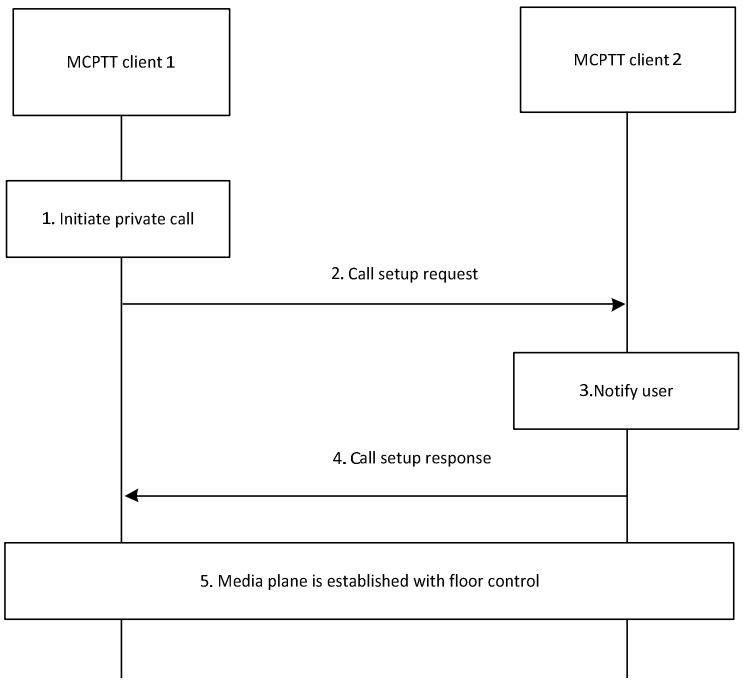

Figure 10.7.3.3-1: Private call setup in automatic commencement mode

1. The MCPTT user at MCPTT client 1 would like to initiate a private call to the MCPTT user at MCPTT client 2.

2. The MCPTT client 1 sends a call setup request towards the MCPTT client 2. The call setup request contains an SDP offer, an automatic commencement mode indication, and an element that indicates that MCPTT client 1 is requesting the floor.

3. The MCPTT client 2 notifies the MCPTT user about the incoming private call.

4. The receiving MCPTT client 2 accepts the private call automatically, and a call setup response indicating the successful call establishment is sent to MCPTT client 1. If MCPTT client 2 rejected the incoming call, the MCPTT client 2 sends a call setup response indicating the failure reason to the MCPTT client 1.

NOTE: Step 4 can also occur prior to step 3.

5. The MCPTT client 1 and the MCPTT client 2 have successfully established the media plane for communication with floor control and the MCPTT client 1 is automatically granted the floor.

10.7.3.4 Private call setup in manual commencement mode

The procedure focuses on the case where an MCPTT user is initiating an MCPTT private call for communicating with another MCPTT user when off-network using a manual commencement mode.

Procedures in figure 10.7.3.4-1 are the basic signalling procedures for the MCPTT client initiating establishment of an off-network MCPTT private call with the chosen MCPTT user.

Pre-conditions:

1. MCPTT user profile used for off-network operation mode is pre-provisioned in the MCPTT UEs.

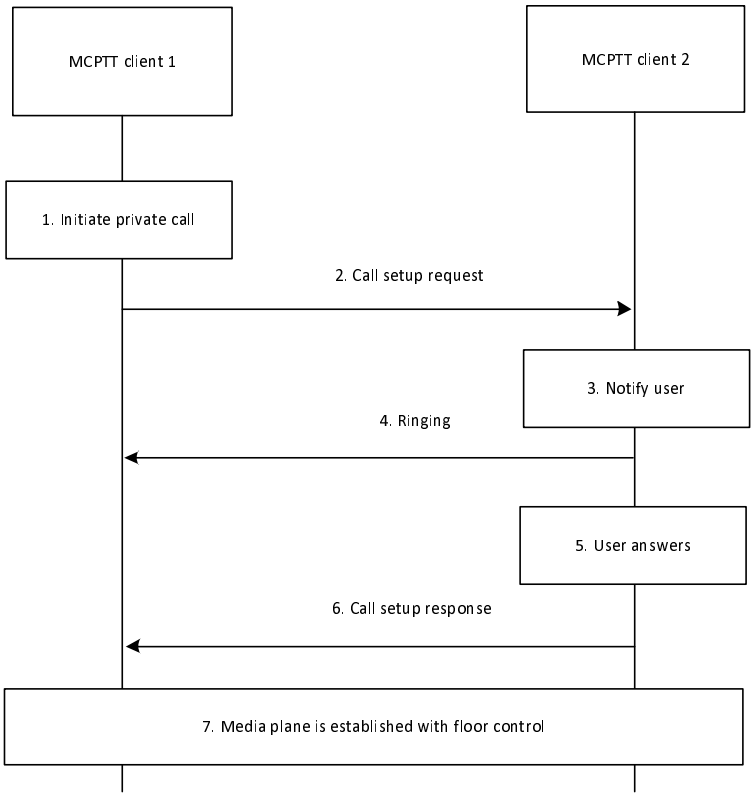

Figure 10.7.3.4-1: Private call setup in manual commencement mode

1. The MCPTT user at MCPTT client 1 would like to initiate an MCPTT private call to the MCPTT user at MCPTT client 2.

2. The MCPTT client 1 sends a call setup request towards the MCPTT client 2. The MCPTT private call setup request contains an SDP offer, a manual commencement mode indication, and an element that indicates that MCPTT client 1 is requesting the floor.

3. The receiving MCPTT client 2 notifies the MCPTT user about the incoming private call.

4. The MCPTT client 2 sends a ringing message to the MCPTT client 1.

NOTE: Step 4 can also occur prior to step 3.

5. The MCPTT user at the MCPTT client 2 has accepted the call using manual commencement mode (i.e., has taken some action to accept via the user interface). The MCPTT user may also reject or fail to answer the incoming call.

6. The MCPTT client 2 sends a call setup response indicating the successful call establishment to MCPTT client 1. If the MCPTT client 2 rejected the call or the MCPTT user 2 rejected or failed to answer the incoming call, the MCPTT client 2 sends a call setup response indicating the failure reason to the MCPTT client 1.

7. The MCPTT client 1 and the MCPTT client 2 have successfully established the media plane for communication with floor control and the MCPTT client 1 is automatically granted the floor.

10.7.3.5 Private call release

The procedure focuses on the case where an MCPTT client is requesting to release an ongoing MCPTT private call whether the call was established using either of the two commencement modes (manual or automatic), as described in subclause 10.7.3.3 and subclause 10.7.3.4. Either MCPTT client can initiate the call release procedure.

Procedures in figure 10.7.3.5-1 are the basic signalling control plane procedures for an MCPTT client initiating the release of an ongoing off-network MCPTT private call.

Pre-conditions:

1. Two MCPTT users are currently engaged in an off-network MCPTT private call.

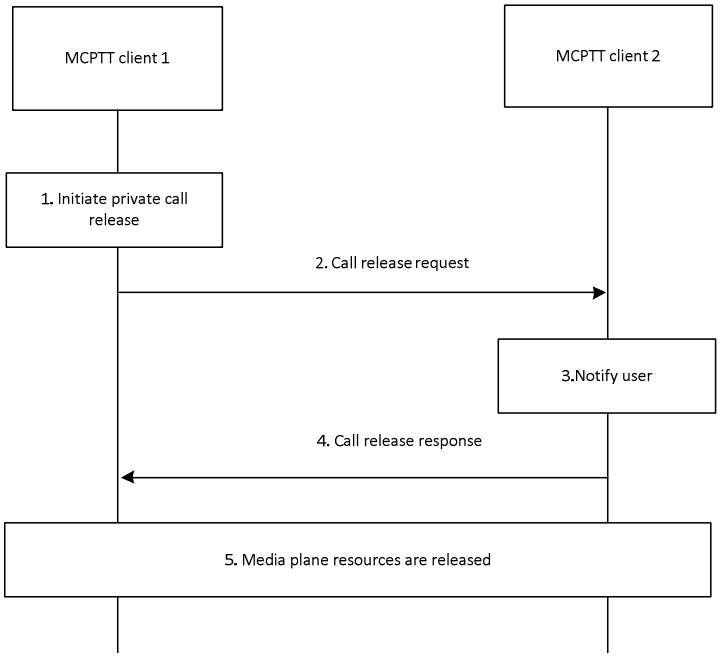

Figure 10.7.3.5-1: Private call release

1. The MCPTT user at MCPTT client 1 would like to initiate an MCPTT private call release to the MCPTT user at MCPTT client 2.

2. The MCPTT client 1 sends a call release request towards the MCPTT client 2.

3. The MCPTT client 2 notifies the MCPTT user about the private call release.

4. The MCPTT client 2 sends a call release response indicating the successful call release to MCPTT client 1.

NOTE: Step 4 can also occur prior to step 3.

5. The MCPTT client 1 and the MCPTT client 2 release all associated media plane resources.

10.7.3.6 MCPTT emergency private call

The off-network emergency private call is a special case of off-network private call as defined in subclause 10.7.3. The following are modifications to the aforementioned subclause to support MCPTT private calls:

- The call setup contains an indication that the MCPTT private call is to be an MCPTT emergency private call,
- the bearers of both MCPTT private call participants are given MCPTT emergency priority prior to media transfer,
- either participant in an MCPTT private call may upgrade the call to the MCPTT emergency state during the call by sending an MCPTT upgrade private emergency request,
- placing an MCPTT emergency private call places the MCPTT client in the MCPTT emergency state,
- the bearer priority of each participant is restored to the priority as it was prior to the MCPTT emergency private call initiation, when the call ends or when the MCPTT emergency priority is cancelled
- an authorized user or the originator of the call may cancel the MCPTT emergency priority of the call by sending an MCPTT cancel private emergency request and
- the MCPTT emergency priority of the MCPTT private call may be cancelled when criteria established by the MCPTT Administrator are met (e.g., timeout).

10.8 Simultaneous session for MCPTT call

10.8.1 General

The simultaneous session for MCPTT call is functionality where the MCPTT client can receive the media from multiple MCPTT calls over the same SIP session and media bearer(s) between the MCPTT client and the MCPTT server.

An MCPTT client becomes involved in simultaneous session for MCPTT calls by inviting, joining or accepting more than one MCPTT call, or affiliating to a group.

NOTE: An MCPTT client affiliating to multiple MCPTT groups with active calls will result in the MCPTT client being invited simultaneously to multiple MCPTT calls.

The MCPTT client can also still handle multiple MCPTT calls in parallel at the same time i.e. using multiple dialogs.

The simultaneous session is established during either an originating on-demand call establishment or during pre-established session establishment or a modification of an already established pre-established session or on-demand call.

It is possible to change the prioritisation while the MCPTT client is engaged in multiple MCPTT calls. The setting of the priority can be made at MCPTT call setup or by performing a modification after the MCPTT call is established. This may result in more than one media bearer.

10.9 Floor control

10.9.1 Floor control for on-network MCPTT service

10.9.1.1 General

The procedure is for providing a floor control to MCPTT UE in an on-network case and applies for both private call and group call. Floor control is performed by using floor control information flows between the floor participant and the floor control server.

10.9.1.2 Information flows for floor control for on-network

10.9.1.2.1 General

When the floor control server receives a floor request from the floor participant, it decides whether to give a grant or not based on, e.g., the session status (i.e., whether the grant is given to another user or not), user profile, priority. The result is informed to the requesting floor participant. When the floor participant receives a floor granted message, it can send voice media over the uplink bearer established beforehand. The floor revoked message can be used as part of override. The floor queue status request can be used to know current position in the queue for floor.

Some floor control information flows can also piggyback call control information flows to provide efficient call setup and clearing:

- Call setup request is optionally carried in floor request (uplink) or floor taken (downlink, can be broadcast); and
- Call release request is optionally carried in floor release (uplink) or floor idle (downlink, can be broadcast).

10.9.1.2.2 Floor request

Table 10.9.1.2.2-1 describes the information flow floor request, from the floor participant to the floor control server, which is used to request the floor for media transfer. This information flow is sent in unicast to the floor control server.

Table 10.9.1.2.2-1: Floor request

Information element	Status	Description
User identity	M	Requester identity
Floor priority	M	Priority of the request
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing

10.9.1.2.3 Floor granted

Table 10.9.1.2.3-1 describes the information flow floor granted, from the floor control server to the floor participant, which is used to indicate that a request for floor is granted and media transfer is possible. This information flow is sent in unicast (to the granted floor participant).

Table 10.9.1.2.3-1: Floor granted

Information element	Status	Description
Duration	M	The time for which the granted party is allowed to transmit
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing
Acknowledgement required	O	Indicates if acknowledgement from the floor participant is required

10.9.1.2.4 Floor rejected

Table 10.9.1.2.4-1 describes the information flow floor rejected, from the floor control server to the floor participant, which is used to indicate that a request for the floor is rejected. This information flow is sent in unicast (to the refused floor participant).

Table 10.9.1.2.4-1: Floor rejected

Information element	Status	Description
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing
Rejection cause	O	Indicates the cause for floor rejection
Acknowledgement required	O	Indicates if acknowledgement from the floor participant is required

10.9.1.2.5 Floor request cancel

Table 10.9.1.2.5-1 describes the information flow floor request cancel, from the floor participant to the floor control server, which is used to request cancelling the floor request from the floor request queue. This information flow is sent in unicast to the floor control server.

Table 10.9.1.2.5-1: Floor request cancel

Information element	Status	Description
User identity	M	Identity for the requester
Target identity(Identities) whose floor request is to be cancelled	M	Identity(ies) of the request(s) to be cancelled.
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing

10.9.1.2.6 Floor request cancel response

Table 10.9.1.2.6-1 describes the information flow floor request cancel response, from the floor control server to the floor control participant, which is used to indicate the response for the floor request cancellation. This information flow is sent in unicast.

Table 10.9.1.2.6-1: Floor request cancel response

Information element	Status	Description
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing
Acknowledgement required	O	Indicates if acknowledgement from the floor participant is required

10.9.1.2.7 Floor request cancel notify

Table 10.9.1.2.7-1 describes the information flow floor request cancel notify, from the floor control server to the floor control participant, which is used to indicate the floor request is cancelled by the administrator/floor control server. This information flow is sent in unicast or broadcast.

Table 10.9.1.2.7-1: Floor request cancel notify

Information element	Status	Description
User identity	M	Identity of the administrator
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing
Acknowledgement required	O	Indicates if acknowledgement from the floor participant is required

10.9.1.2.8 Floor idle

Table 10.9.1.2.8-1 describes the information flow floor idle, from the floor control server to the floor participant, which is used to indicate that a session is in idle status, i.e. the floor is not granted to any party. This information flows is sent in unicast or broadcast.

Table 10.9.1.2.8-1: Floor idle

Information element	Status	Description
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing
Acknowledgement required	O	Indicates if acknowledgement from the floor participant is required

10.9.1.2.9 Floor release

Table 10.9.1.2.9-1 describes the information flow floor release, from the floor participant to the floor control server, which is used to indicate the media transfer is completed and floor is released. This information flow is sent in unicast to the floor control server.

Table 10.9.1.2.9-1: Floor release

Information element	Status	Description
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing

10.9.1.2.10 Floor taken

Table 10.9.1.2.10-1 describes the information flow floor taken, from the floor control server to the floor participant, which is used to indicate the floor is granted to another MCPTT user. This information flows is sent in unicast or broadcast.

Table 10.9.1.2.10-1: Floor taken

Information element	Status	Description
User identity	M	Identity for the granted party
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing
Permission to request the floor	O	Indicates whether receiving parties are allowed to request the floor or not (e.g. broadcast call).
Acknowledgement required	O	Indicates if acknowledgement from the floor participant is required

10.9.1.2.11 Floor revoked

Table 10.9.1.2.11-1 describes the information flow floor revoked, from the floor control server to the floor participant, which is used to indicate the floor is revoked from its current holder (the floor participant who was granted the floor). This information flows is sent in unicast (to the revoked floor participant).

Table 10.9.1.2.11-1: Floor revoked

Information element	Status	Description
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing
Acknowledgement required	O	Indicates if acknowledgement from the floor participant is required

10.9.1.2.12 Floor acknowledgement

Table 10.9.1.2.12-1 describes the information flow floor acknowledgement, from the floor participant to the floor control server, which is used to provide an acknowledgement if the acknowledgement is required in the received floor control message.

Table 10.9.1.2.12-1: Floor acknowledgement

Information element	Status	Description
User identity	M	Identity of the sender.

10.9.1.2.13 Queue position request

Table 10.9.1.2.13-1 describes the information flow queue position request, from the floor participant to the floor control server, which is used to request the position in the floor request queue. The MCPTT server and the MCPTT client support queuing of the floor control requests shall support this information flow. This information flow is sent in unicast to the floor control server.

Table 10.9.1.2.13-1: Queue position request

Information element	Status	Description
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing

10.9.1.2.14 Queue position info

Table 10.9.1.2.14-1 describes the information flow queue position request, from the floor control server to the floor participant, which is used to indicate the floor request is queued and the queue position to the floor requesting UE. The MCPTT server and the MCPTT client support queuing of the floor control requests shall support this information flow. This information flows is sent in unicast (to the queued floor participant).

Table 10.9.1.2.14-1: Queue position info

Information element	Status	Description
Queue position info	M	Position of the queued floor request in the queue
Source identifier	O	Identifies the communication, e.g. by identifying the media flow within a media multiplex, present only in case of media multiplexing
Acknowledgement required	O	Indicates if acknowledgement from the floor participant is required

10.9.1.3 Floor control within one MCPTT system

10.9.1.3.1 Floor request, floor granted and floor taken during an MCPTT session

Figure 10.9.1.3.1-1 shows the high level procedure that the floor control is conducted for the MCPTT session already established between the floor participant and the floor control server. Only two UEs involved in the session are shown for the simplicity.

Pre-condition:

1. MCPTT session is established between MCPTT clients (client A and client B) and MCPTT server.

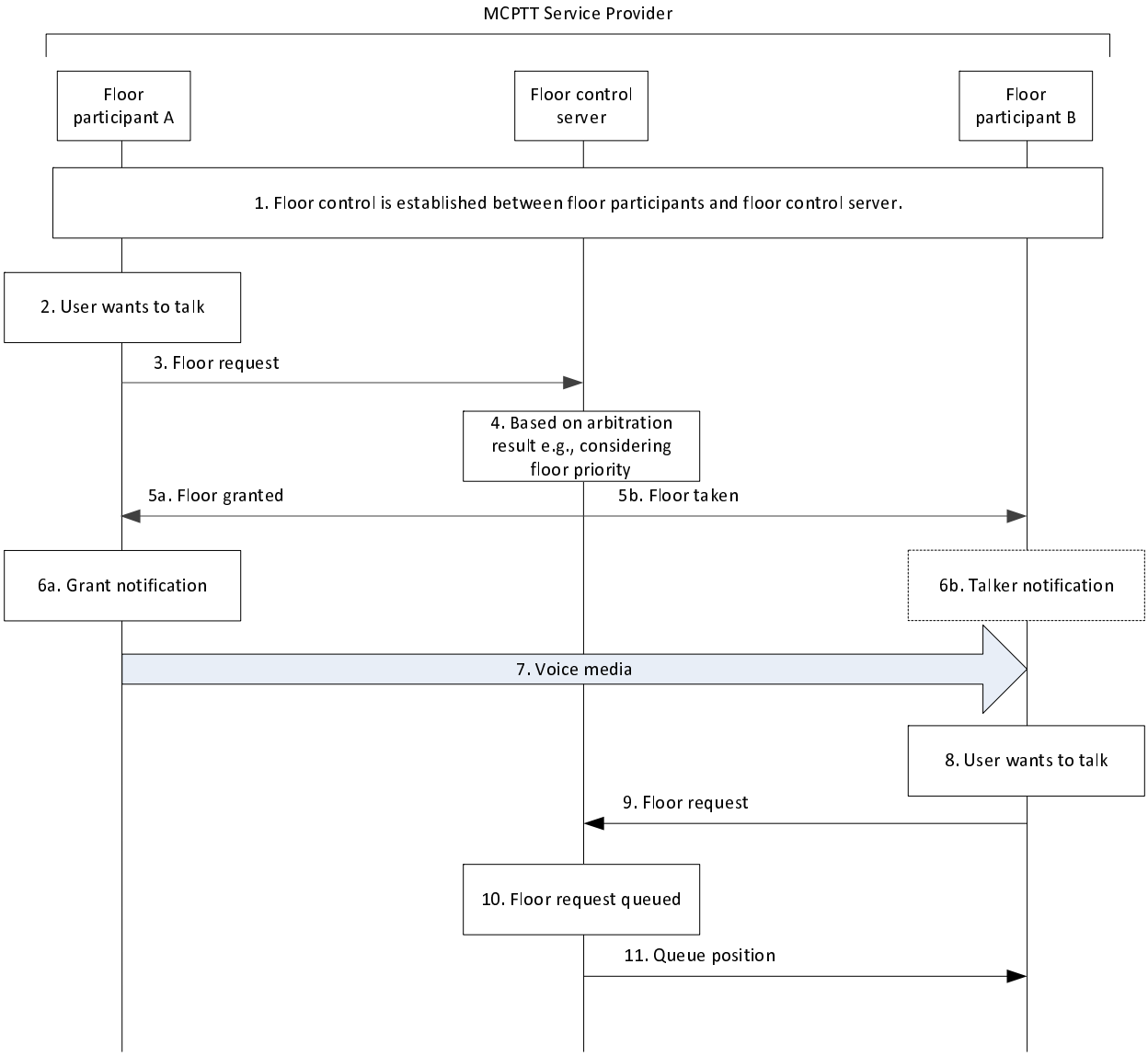

Figure 10.9.1.3.1-1: Floor request, floor granted, floor taken during an MCPTT session

1. The floor control is established between the floor participants and floor control server. It is assumed that the floor is now in idle status.
2. Floor participant A wants to send voice media over the session.
3. Floor participant A sends a floor request message to floor control server which includes floor priority and other information as necessary.

4. Floor control server makes the determination on what action (grant, deny, or queue) to take on the request based on criteria (e.g., floor priority) and determines to accept the floor request from floor participant A. The floor control server may limit the time a user talks (hold the floor) as allowed by the configuration.

5a. Floor control server responds with a floor granted message to floor participant A including the maximum floor granted duration e.g., if no other floor participant has the permission for transmission.

5b. Floor control server sends a floor taken message to the other floor participant (floor participant B) including information about who is granted the floor.

6a. The floor granted shall cause the user of UE A where the floor participant A is located to be notified.

6b. The receipt of the floor taken may be used to inform the user of UE B where the floor participant B is located.

7. Floor participant A starts sending voice media over the session established beforehand.

NOTE: Voice media can continue to be sent while steps 8 through 11 occur.

8. Suppose there are one or more users requesting to talk at this time, the floor request(s) are queued as decided by floor control server e.g., based on floor priority.

9. Floor participant B sends a floor request message.

10. Floor control server queues the request of floor participant B.

11. Floor control server sends queue position info to floor participant B.

10.9.1.3.2 Floor override

10.9.1.3.2.1 Floor override using floor revoked (also floor rejected) during an MCPTT session

Figure 10.9.1.3.2.1-1 shows the high level procedure that the floor control is conducted for the MCPTT session already established between the floor participant (with floor granted to floor participant B) and the floor control server (with an override based on priority). Only two UEs involved in the session are shown for the simplicity.

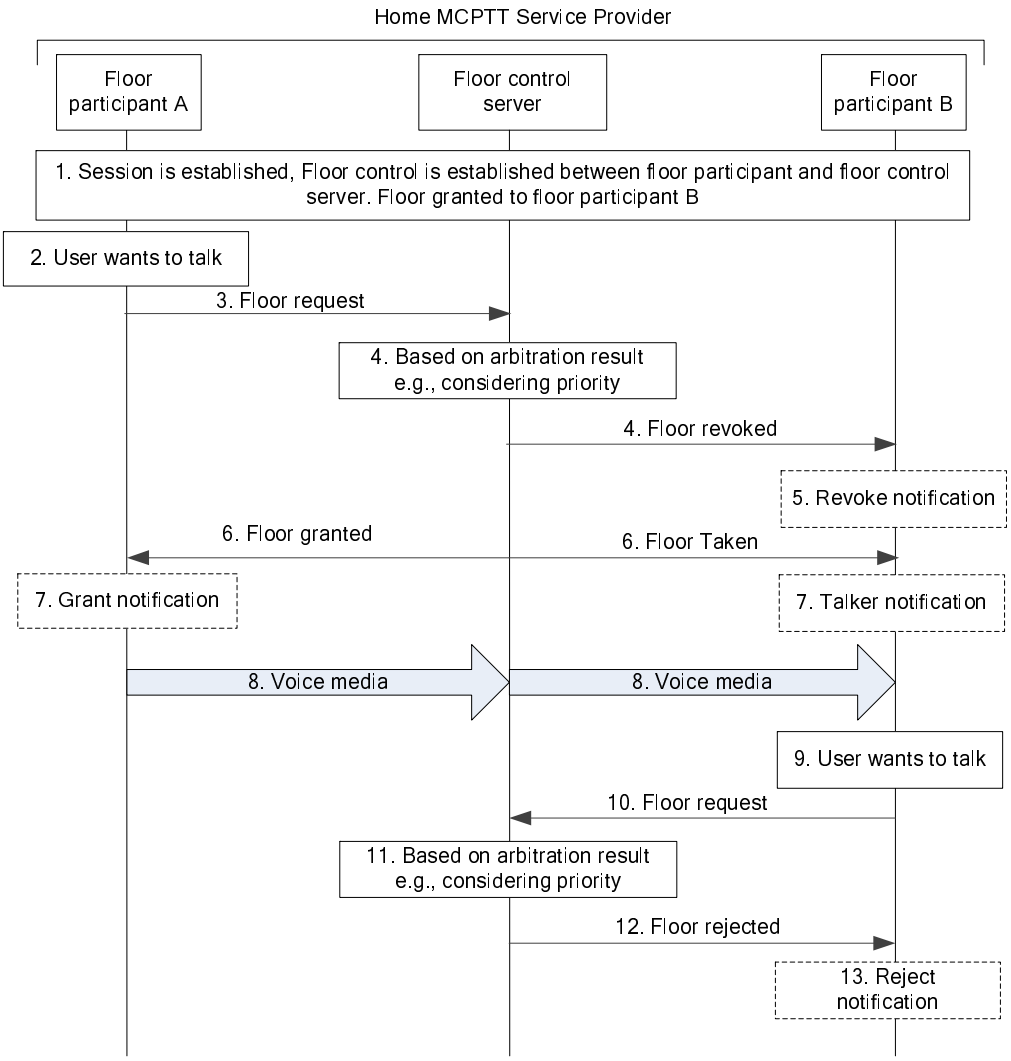

Figure 10.9.1.3.2.1-1: Floor override using floor revoked (also floor rejected) during an MCPTT session

1. It is assumed that floor participant B has been given floor and is transmitting voice media.
2. Floor participant A having a priority which is relatively higher than that of floor participant B wants to send voice media over the session.
3. Floor participant A sends a floor request message to the floor control server.
4. The floor control server determines to accept the floor request from floor participant A based on arbitration result e.g., according to the priority information that is received in the floor request message. The floor control server sends a floor revoked message to floor participant B stopping the voice media transmission from floor participant B.
5. The user of floor participant B may be notified that the floor is revoked.
6. The Floor control server sends a floor granted message to floor participant A, while sending a floor taken message to floor participant B with information of who is granted the floor.
7. The user of floor participant A may be notified that he is granted the floor. Similarly, the user of floor participant B may be notified who is granted the floor.
8. Floor participant A starts sending voice media over the session established beforehand.
9. Now floor participant B may want the floor to start sending voice media.
10. Floor participant B sends a floor request message to floor control server which may include priority information.

11. Floor control server determines whether to accept the floor request from floor participant B based on arbitration result e.g., according to the priority information that is received in the floor request message.

12. The floor control server responds with a floor rejected message to floor participant B.

13. Floor participant B may be notified that he is rejected.

10.9.1.3.2.2 Floor override without using floor revoked during an MCPTT session

Figure 10.9.1.3.2.2-1 shows the high level procedure that the floor control is conducted for the MCPTT session already established between the floor participants (with floor granted to floor participant B) and the floor control server (with an override based on priority and configured to permit the transmission of the overridden floor participant B to continue). Only two UEs involved in the session are shown for the simplicity.

Pre-conditions

- The floor control server has been configured to support override.
- The override supported in this case permits both the overridden floor participant and the overriding floor participant to be transmitting.

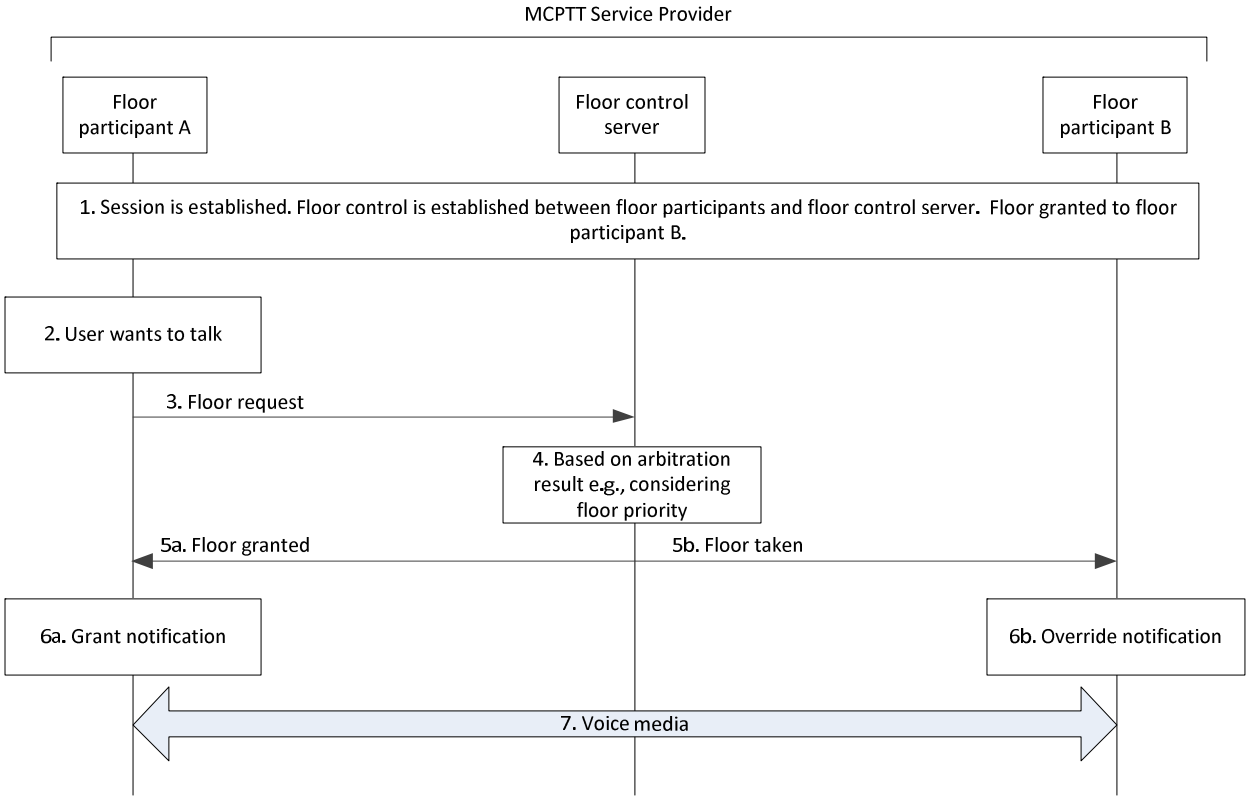

Figure 10.9.1.3.2.2-1: Floor override (overridden continues to transmit) during an MCPTT session

1. It is assumed that floor participant B has been given the floor and is transmitting voice media.

2. Floor participant A having a floor priority which is relatively higher than that of floor participant B wants to send voice media over the session.

3. Floor participant A sends a floor request message to the floor control server.

4. The floor control server determines to accept the floor request from floor participant A based on arbitration result e.g., according to the floor priority information that is received in the floor request message.

5a. Floor control server responds with a floor granted message to floor participant A.

5b. Floor control server sends a floor taken message to the other floor participants (including floor participant B). Floor participant B continues transmitting the (overridden) voice media transmission.

NOTE 1: All other floor participants (not shown) that are part of this group call receive a floor taken message, so that the other floor participants learn who the newly granted talker (overriding) is.

6a. The floor granted causes the user of floor participant A to be notified.

6b. The user of floor participant B is notified of the status that the floor is now taken by floor participant A.

7. Floor participant A (overriding) starts sending voice media over the session established beforehand.

NOTE 2: Floor participant B is still sending voice (overridden). The list of floor participants that receive the overriding, overridden, or both transmissions is based on configuration.

10.9.1.3.3 Queue position during an MCPTT session

Figure 10.9.1.3.3-1 shows the high level procedure that the floor control is conducted for the MCPTT session already established between MCPTT clients (with floor granted to floor participant B) and server (with an override based on priority at floor control server). Only two UEs involved in the session are shown for the simplicity.

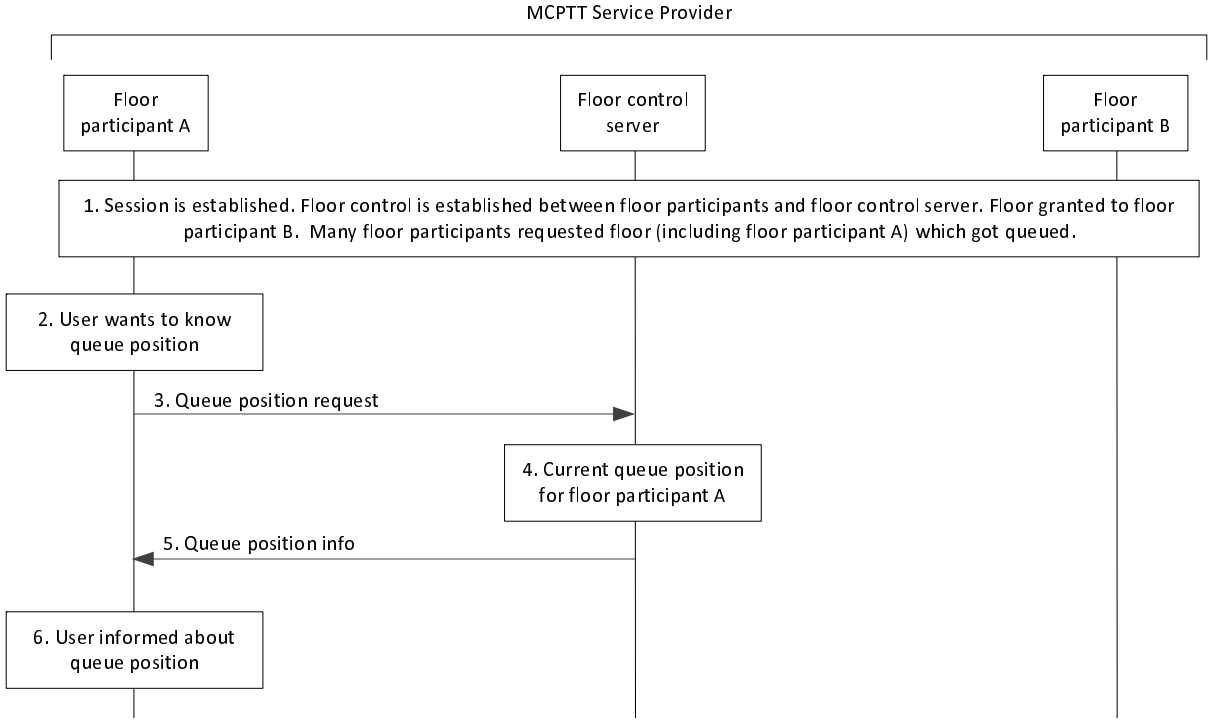

Figure 10.9.1.3.3-1: Queue status during an MCPTT session

1. It is assumed that floor participant B has been given a floor granted and is transmitting voice media. There are several other floor participants (including floor participating A) requesting floor which get queued at the floor control server.
2. Floor participant A would like to know its current position in the floor request queue.
3. Floor participant A sends a queue position request message to the floor control server.
4. Floor control server determines the current queue position of floor participant A from the floor request queue.
5. Floor control server responds with the current position in queue position info message.
6. User at floor participant A is informed about the current queue position.

10.9.1.3.4 Floor request cancellation from the floor request queue

10.9.1.3.4.1 Floor request cancellation from the queue – MCPTT user initiated

Figure 10.9.1.3.4.1-1 illustrates the procedure for floor request cancellation from the floor queue initiated by the MCPTT user. The MCPTT user may be an authorized user who has rights to cancel the floor requests of other MCPTT users, whose floor requests are in floor control queue.

Pre-conditions:

- It is assumed that floor participant B has been granted the floor and is transmitting voice media. There are several other floor participants (including floor participant A and floor participant C) requesting the floor which have been queued at the floor control server.

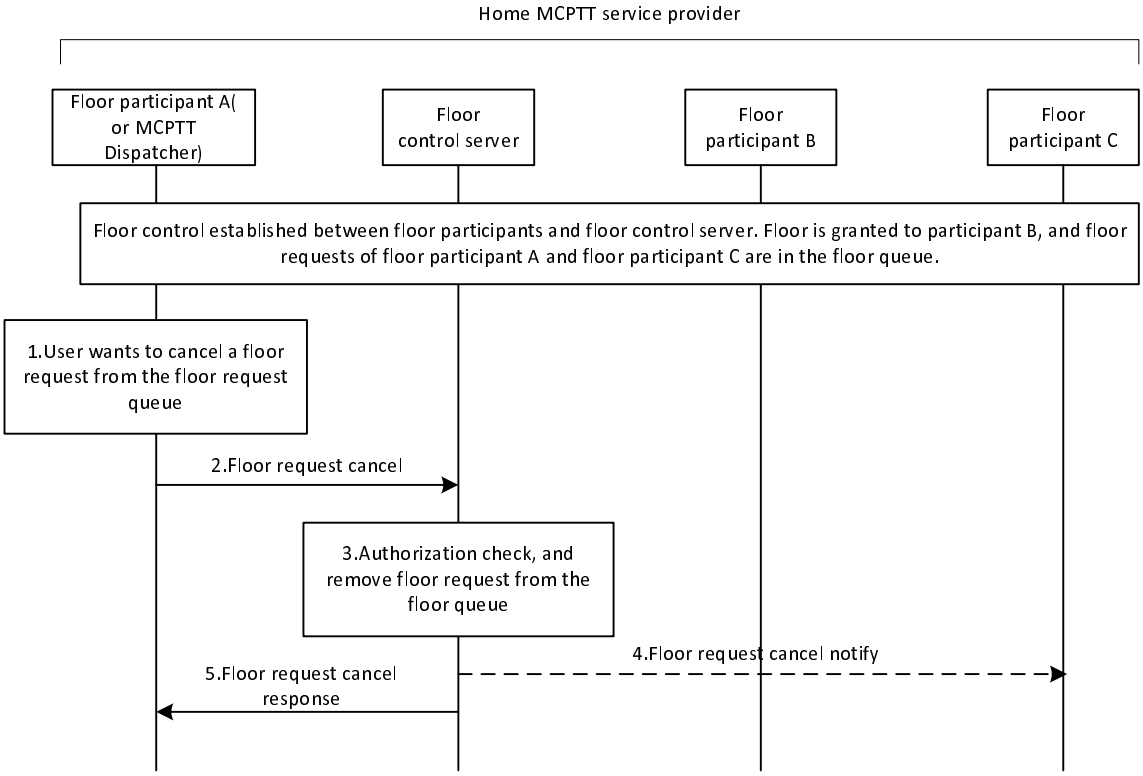

Figure 10.9.1.3.4.1-1: Floor request cancellation from queue initiated by MCPTT user

1. The floor participant A wants to remove the floor request from the floor request queue. If floor participant A is an authorized MCPTT user with the rights to cancel another MCPTT user's floor request, the authorized MCPTT user may request floor request cancellation for one or more floor participants, whose floor request needs to be removed from the floor queue.

2. The floor participant A sends a floor request cancel (initiating MCPTT user ID) message to the floor control server. If the floor participant A wants to remove the floor request(s) of other participant(s), the target participant(s)' MCPTT user ID should be included in this message.

3. The floor control server shall check whether the requesting floor participant has authorization to cancel the floor request(s). If authorized, the floor request(s) will be removed from the floor request queue. When current transmission is completed, floor control server will process the floor request from the updated floor request queue.

4. If the floor request cancel in step 3 is sent by an authorized user (e.g., dispatcher) to cancel the floor request(s) of other participant(s) from the floor request queue, the floor request cancel notify message is sent to the floor participant whose floor request was cancelled from the floor queue.

5. The floor control server provides a floor request cancel response to the floor participant A when the floor cancellation is completed. Optionally, the new queue position information may be notified to the floor participants whose floor requests are in the floor request queue (not shown in the figure).

10.9.1.3.4.2 Floor request cancellation from the queue - floor control server initiated

Figure 10.9.1.3.4.2-1 illustrates the procedure for floor request cancellation from the queue initiated by the floor control server. Only two UEs involved in the session are shown for the simplicity.

Pre-conditions:

- It is assumed that floor participant B has been granted the floor and is transmitting voice media. There are several other floor participants (including floor participant A and participant C) requesting the floor which have been queued at the floor control server.

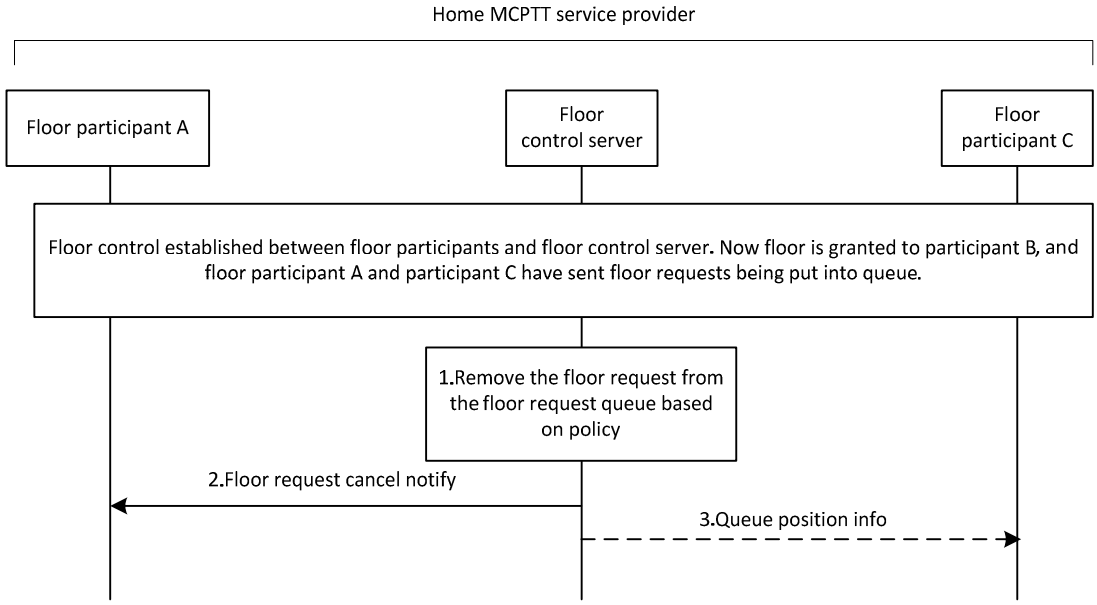

Figure 10.9.1.3.4.2-1: Floor request cancellation from queue initiated by floor control server

1. The floor control server removes the floor request from the floor request queue based on policy. e.g., expiration of a timer. In the case when floor control server receives repeated floor requests from a floor participant while the floor is occupied, the new floor request is accepted and added into the floor queue and the existing/former floor request is removed from the floor queue or the new floor request is rejected and the existing/former floor request of this floor participant is retained in the floor request queue.

2. The floor control server sends a floor request cancel notify to the floor participant(s) whose floor request is removed from the floor request queue.

3. Optionally, the newly queue position information is notified to the other floor participants whose floor requests are queued.

10.9.1.4 Floor control involving groups from multiple MCPTT systems

10.9.1.4.1 Partner MCPTT system routes all floor control messages to primary MCPTT system's floor control server

The MCPTT users belonging to different groups in multiple MCPTT systems will participate in MCPTT media services (group communication, private calls, etc.) in scenarios like group hierarchies and temporary groups formed by group regroup. In this service delivery model involving multiple groups from different MCPTT systems, the floor control arbitration resides with the primary MCPTT system. This is determined in the group call setup stage. The MCPTT users of groups involved in the call session will transmit their floor control messages through the partner MCPTT systems to which they belong. In this scenario, the partner MCPTT systems request the floor control for its MCPTT user(s) from

the floor control server of the primary MCPTT system. The protocol used for media plane signalling is non-SIP like RTCP.

Figure 10.9.1.4.1-1 describes the procedure for floor control involving groups from multiple MCPTT systems.

Pre-conditions:

1. The security aspects of sharing the user information between primary and partner MCPTT systems shall be governed as per the service provider agreement between them. In this case, we consider the partner MCPTT system does not share all information of their users' to the primary MCPTT system (public information would still need to be shared).

2. The group 1 is hosted by primary MCPTT system and group 2 and 3 are hosted by the partner MCPTT system.

3. The floor participant 1 corresponds to the MCPTT user of group 1. The floor participant 2 corresponds to the MCPTT user of group 2. The floor participant 3 corresponds to the MCPTT user of group 3. The floor control server 1 belongs to primary MCPTT system. The floor control server 2 belongs to partner MCPTT system.

4. The floor control server 1 is the floor arbitrator of the MCPTT group call. The floor control server 2 routes all floor control messages to and from the floor participants 2 and 3 and then floor control server 1.

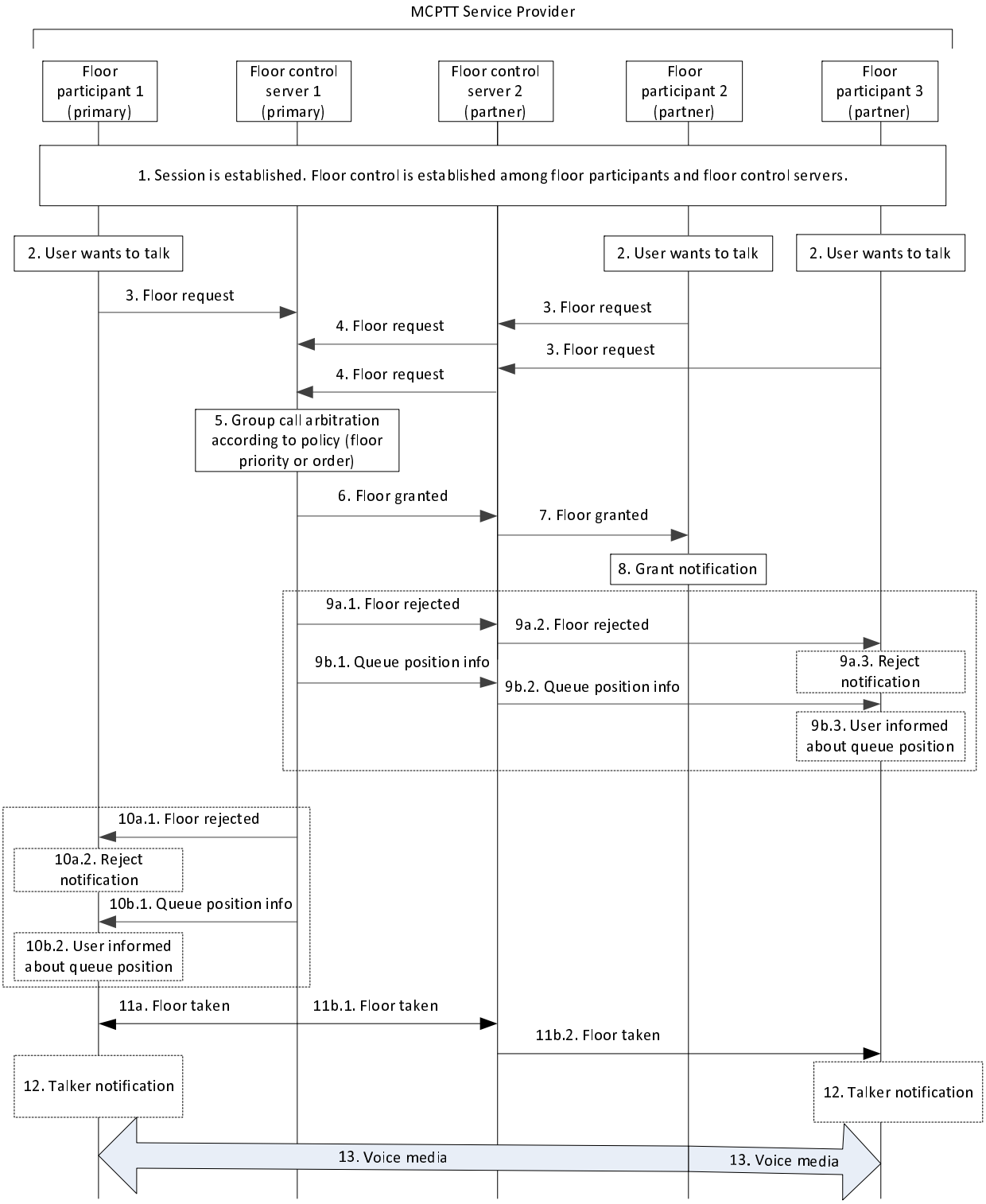

Figure 10.9.1.4.1-1: Floor control (partner MCPTT system forwarding) involving groups from multiple MCPTT systems

1. An MCPTT group call involving group1, group 2 and group 3 is setup and active.
2. The MCPTT users want to talk.
3. The floor participants initiate a floor request to the floor control server of their corresponding MCPTT systems. (The requests may or may not occur at the same time).
4. If only one floor request is received, or floor control server 2 handles the floor request sequentially, there is no arbitration performed and the corresponding floor request is forwarded to the floor control server 1. If the floor

control server 2 receives multiple floor requests at the same time or during an interval, then it forwards the floor requests to the floor control server 1 (floor arbitrator for the MCPTT group call). As the floor participant information shall not be exposed, the floor priority related information or/and group information to be used by floor control server 1 should be included in the forwarded request.

5. The floor control server 1 performs floor arbitration for the MCPTT group call and determines the floor request to be accepted.

6. If the floor request from floor participant 2 of the partner MCPTT system is accepted, a floor granted is sent with permission to talk. The floor control messages from floor control server 1 are routed to floor participant 2 via the floor control server 2.

7. When the floor control server 2 (partner) receives the floor granted, the floor control server 2 sends a floor granted message on to floor participant 2.

8. The floor granted shall cause the user of the UE where the floor participant 2 is located to be notified.

9. The primary floor control server 1 may (9a.1) send a floor rejected message, or (9b.1) send a queue position info message for each non-granted received floor requests forwarded from the floor control server 2 (partner). When the floor control server 2 (partner) receives the floor rejected message, then the floor control server 2 (partner) (9a.2) sends a floor rejected message to the appropriate floor participant. When the floor control server 2 (partner) receives the queue position info, then the floor control server 2 (partner) (9b.2) sends a queue position info message to the appropriate floor participant.

10a.1 If floor control server 1 rejects the floor request from floor participant 1, then a floor reject message is sent.

10a.2 Upon this being received the user of the UE where floor participant 1 is located may be notified.

10b.1 If floor control server 1 supports floor queue, queue position info message is sent to the floor participant 1.

10b.2 Upon this being received the user of the UE where floor participant 1 is located may be notified.

NOTE 1: Steps 10a.1 through 10.b2 are optional as indicated by the dashed box enclosing them. However if this box is implemented then either information flow 10a or 10b would occur.

11. Since the floor is granted to floor participant 2 of the partner MCPTT system, then a floor taken is sent to all other floor participants ((11a) floor participant 1 and (11b.1) to floor control server 2 (partner) for forwarding to (11b.2) floor participant 3.

12. The receipt of the floor taken may be used to inform the users of the UEs where the floor participant entity 1 and floor participant 3 are located to be notified.

13. Upon successful floor granted, the group call media transmission occurs.

NOTE 2: The media flow between the media gateways of primary and partner MCPTT systems have not been depicted in the figure for clarity.

10.9.1.4.2 Partner MCPTT system performs filtering of floor control messages entering and leaving the partner MCPTT system

The MCPTT users belonging to different groups in multiple MCPTT systems will participate in MCPTT media services (group communication, private calls, etc.) in scenarios like group hierarchies and temporary groups formed by group regroup. In this service delivery model involving multiple groups from different MCPTT systems, the floor control arbitration resides with the primary MCPTT system. This is determined in the group call setup stage. The MCPTT users of groups involved in the call session will transmit their floor control messages through the partner MCPTT systems to which they belong. In this scenario, the partner MCPTT system filters its MCPTT users' floor requests before communicating with the floor control server of the primary MCPTT system. The protocol used for media plane signalling is non-SIP like RTCP.

Figure 10.9.1.4.2-1 describes the procedure for floor control involving groups from multiple MCPTT systems.

Pre-conditions:

1. The security aspects of sharing the user information between primary and partner MCPTT systems shall be governed as per the service provider agreement between them. In this case, we consider the partner MCPTT

system does not share all information of their users to the primary MCPTT system (public information would still need to be shared).

2. The group 1 is hosted by primary MCPTT system and group 2 and 3 are hosted by the partner MCPTT system.

3. The floor participant 1 corresponds to the MCPTT user of group 1. The floor participant 2 corresponds to the MCPTT user of group 2. The floor participant 3 corresponds to the MCPTT user of group 3. The floor control server 1 belongs to primary MCPTT system. The floor control server 2 belongs to partner MCPTT system.

4. The floor control server 1 is the floor arbitrator of the MCPTT group call. The floor control server 2 does floor control filtering with its floor participants 2 and 3 before communicating with the floor control server 1.

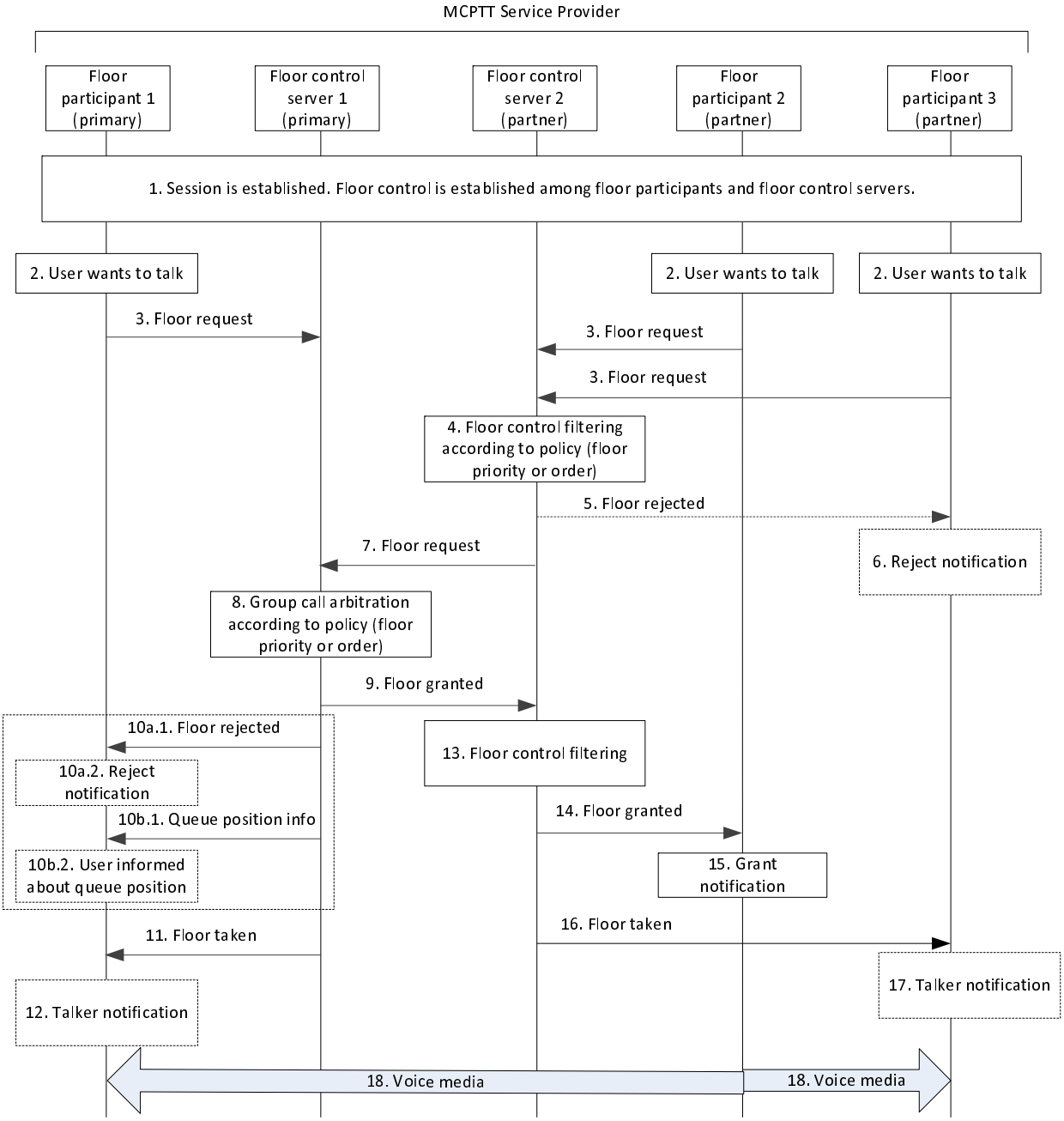

Figure 10.9.1.4.2-1: Floor control (filtering by partner MCPTT system) involving groups from multiple MCPTT systems

1. An MCPTT group call involving group 1, group 2 and group 3 is setup and active.

2. The MCPTT users want to talk

3. The floor participants initiate a floor request to the floor control server of their corresponding MCPTT systems. (The requests may or may not occur at the same time).

4. Floor control server 2 receives a floor request from floor participant 2 and from participant 3 at the same time or during an interval, then the floor control server 2 (partner) performs filtering of the floor requests received according to its local policy such as priority or order based on its own users, and forwards the selected floor request (floor participant 2) to the floor control server 1 (floor arbitrator for the MCPTT group call). As the floor participant information shall not be exposed, the priority related information or/and group information to be used by floor control server 1 should be included in the forwarded request.

5. The floor control server 2 (partner) may send a floor rejected towards the floor participant 3, since its floor request was not chosen to be forwarded on to the floor control server 1.

6. The user on the UE where the floor participant 3 is located may be notified of the rejection.

NOTE 1: Steps 5 and 6 can occur any time between step 4 and step 16.

7. The floor control server 2 (partner) forwards the floor request of floor participant 2 to the floor server 1.

8. The floor control server 1 performs floor arbitration for the MCPTT group call and determines the floor request to be accepted. The floor request message from floor participant 2 of the partner system is accepted by the floor control server 1 (arbitrator) and is determined that a floor granted is sent with permission to talk.

9. The floor granted message from floor control server 1 is routed to floor participant 2 via the floor control server 2 (partner).

10. Since floor participant 1 sent a floor request but was not granted,

10a.1 the primary floor control server may send a floor rejected message to floor participant 1.

10a.2 The user of the UE where the floor participant 1 is located may be notified of the rejection.

10b.1 if floor control server supports floor queuing, send a queue position info message to floor participant 1.

10b.2 The user of the UE where the floor participant 1 is located may be notified of the queue position.

NOTE 2: Steps 10a.1 through 10.b2 are optional as indicated by the dashed box enclosing them. However if this box is implemented then either information flow 10a or 10b would occur.

11. A floor taken message is sent to floor participant 1.

12. The user of the UE where the floor participant 1 is located may be notified.

NOTE 3: Step 10 through Step 12 can occur any time between step 8 and step 18.

13. Since the floor control server 2 (partner) filters floor requests, when the floor control server 2 (partner) receives the floor granted for floor participant 2 from floor control server 1, the floor control server 2 (partner) needs to use the information received to generate the floor taken which will be sent to all other floor participants (floor control participant 3).

14. The floor control server 2 (partner) sends a floor granted message to floor participant 2.

15. The user of the UE where the floor participant 2 is located is notified.

16. The floor control server 2 (partner) sends a floor taken message to all other floor participants (floor participant 3).

17. The user of the UE where the floor participant 1 is located may be notified.

18. Upon successful floor grant, the group call media transmission occurs.

NOTE 4: The media flow between the media gateways of primary and partner MCPTT systems have not been depicted in the figure for clarity.

10.9.2 Floor control for off-network MCPTT service

10.9.2.1 General

The procedures defined in this subclause provide floor control to MCPTT UEs in off-network operation. The procedures apply to both private calls and group calls.

In off-network, floor control is performed by using floor control messages among the MCPTT clients without centralized MCPTT server. The MCPTT client can transmit voice packets once it is granted the right to speak, either locally in the UE or by reception of a floor granted message from another MCPTT client.

In off-network, the MCPTT client currently speaking performs the temporary floor arbitrator during speaking since there is no centralized MCPTT floor control server. The floor arbitrator controls the floor whether or not queue is supported, and when floor is requested with override. If queue is supported, the MCPTT client performing floor arbitrator grants the right to speak to the next speaker and transfers the floor arbitrator role after completing the voice transfer and releasing the floor. For group calls, the floor arbitrator also transfers the floor control queue when granting the floor. The next MCPTT client receiving the right to speak becomes the new floor arbitrator and, for group calls, has the floor control queue.

For group calls, the floor control message is delivered in multicast based communication and can be monitored by all the members within the MCPTT group.

The following information flows apply among MCPTT clients.

- Floor request (from the floor participants to the floor arbitrator): used to request a floor for voice transfer.
- Floor release (from the floor arbitrator to the floor participants): used to inform that the voice transfer is completed and the floor is released.
- Floor granted (from the floor arbitrator to a floor participant): used to indicate that the request for floor is granted, that voice transfer is possible and the current queue list.
- Queue position request (from the floor participant to the floor arbitrator): used to request the position in the floor request queue.
- Queue position info (from the floor arbitrator to the floor participant): used to indicate the floor request is queued and the current queue status.
- Floor rejected (from the floor arbitrator to the floor participant): used to indicate that a request for the floor is rejected.

10.9.2.2 Information flows for floor control for off-network

10.9.2.3 Floor control during silence

10.9.2.3.1 Successful floor taken (No floor contention)

If a floor arbitrator still exists, the expected behaviour for floor requests during periods of silence is described in subclauses 10.9.2.5 and 10.9.2.6 represent (with the exception that no media was being generated prior to the floor request).

If a floor arbitrator does not exist, figure 10.9.2.3.1-1 shows the successful high level floor control procedure during periods when there is no detectable talker.

NOTE 1: The description also applies to private calls.

Pre-conditions:

1. An off-network group call had been established and all MCPTT clients have the call parameters. No participant is currently talking and no floor arbitrator is identified.

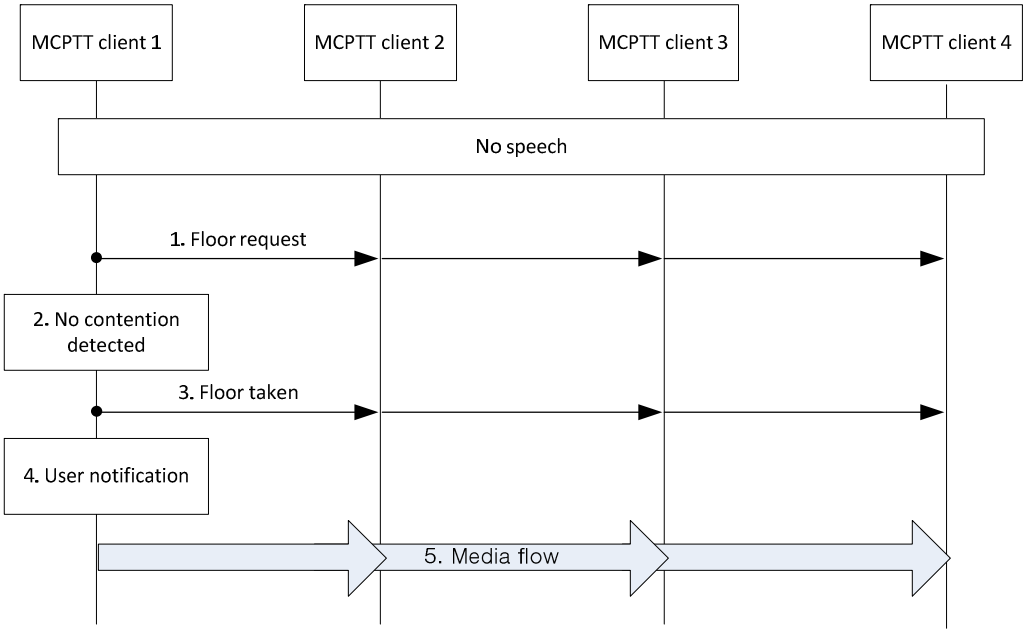

Figure 10.9.2.3.1-1: Successful floor taken flow (No floor contention)

1. The MCPTT client 1 sends the floor request message to the MCPTT group.
2. The MCPTT client 1 does not detect any floor contention. Floor contention occurs when multiple floor requests may exist simultaneously.

NOTE 2: The mechanism for detecting floor contention is out of scope of the present document.

3. The MCPTT client 1 sends the floor taken message to the MCPTT group.
4. The user gets a notification that the floor request was successful (the floor has been granted).
5. The MCPTT client 1 begins voice transmission.

10.9.2.4 Simultaneous floor requests

10.9.2.5 Floor request during speaking with queue

Figure 10.9.2.5-1 shows the high level procedure that the floor control is conducted when the MCPTT off-network session is already established among MCPTT floor participants and while voice media is transmitting. In the case, MCPTT clients should support queue function. The current speaking MCPTT client acting as the floor arbitrator put the floor request into the queue list when receiving the floor request from other MCPTT clients. This procedure happens while voice media is transmitting. In the flow, MCPTT client 1 transmits the voice media to the MCPTT group and acts as the floor arbitrator.

NOTE: The description only applies to group calls.

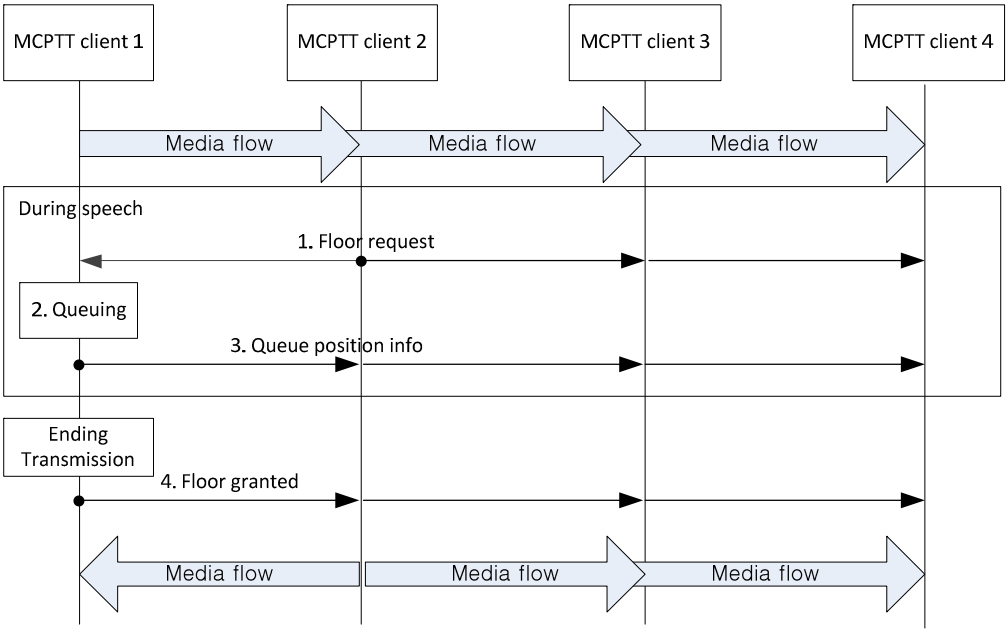

Figure 10.9.2.5-1: Floor request during speaking with queue

1. MCPTT client 2 sends the floor request message to the MCPTT group.
2. MCPTT client 1 acting as the floor arbitrator put the floor request of MCPTT client 2 into the queue list.
3. MCPTT client 1 sends the queue position info message with the queuing status regarding the floor request of MCPTT client 2 in order to inform the floor request is queued.
4. MCPTT client 1 sends the floor granted message to the MCPTT group when releasing the floor. The message contains the MCPTT ID to be granted to send the voice media, and queue list, if any. MCPTT client 1 may include the maximum duration that MCPTT client 2 transmits in the floor granted message.
5. MCPTT client 2 sends the voice media when receiving the floor granted message and being granted as next speaker in the floor granted message. In addition, MCPTT client 2 becomes the floor arbitrator.

10.9.2.6 Floor request during speaking without queue

Figure 10.9.2.6-1 shows the high level procedure that the floor control is conducted when the MCPTT off-network session is already established among MCPTT floor participants. In the case, MCPTT clients do not support queue function. The current speaking MCPTT client acting as the floor arbitrator controls the floor request when receiving the floor request from other MCPTT clients. This procedure happens while voice media is transmitting. In the flow, MCPTT client 1 transmits the voice media to the MCPTT group and acts as the floor arbitrator.

NOTE: The description also applies to private calls.

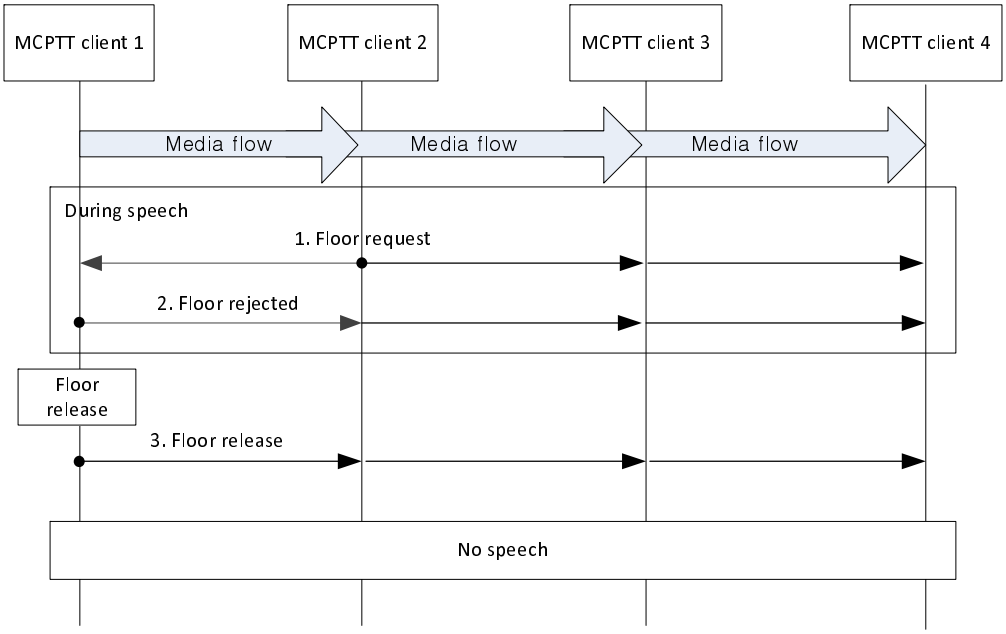

Figure 10.9.2.6-1: Floor request during speaking without queue

1. MCPTT client 2 sends the floor request message to the MCPTT group.
2. MCPTT client 1 acting as the floor arbitrator rejects the floor request from MCPTT client 2 if no queue function is supported and sends the floor rejected message to the MCPTT group.
3. MCPTT client 1 sends the floor release message to the MCPTT group when releasing the floor, in order to indicate that MCPTT client 1 finishes to send the voice media and releases the floor.

   When the floor release message is transmitted, there are no voice media in the MCPTT group until an MCPTT client requests the floor as described in subclause 10.9.2.3.

10.9.2.7 Override

Figure 10.9.2.7-1 shows the high level procedure that the floor control is conducted when the MCPTT off-network session is already established among MCPTT floor participants and while voice media is transmitting. When the currently speaking MCPTT floor participant receives the floor request message from another floor participant who is authorized to revoke the active transmission (e.g. higher hierarchy), the current speaking MCPTT floor participant immediately stops sending the audio media and then grants the permission to that authorized floor participant.

NOTE: The description also applies to private calls.

Pre-condition:

- MCPTT client 1, who acts as the floor arbitrator, transmits the audio media to the MCPTT group.

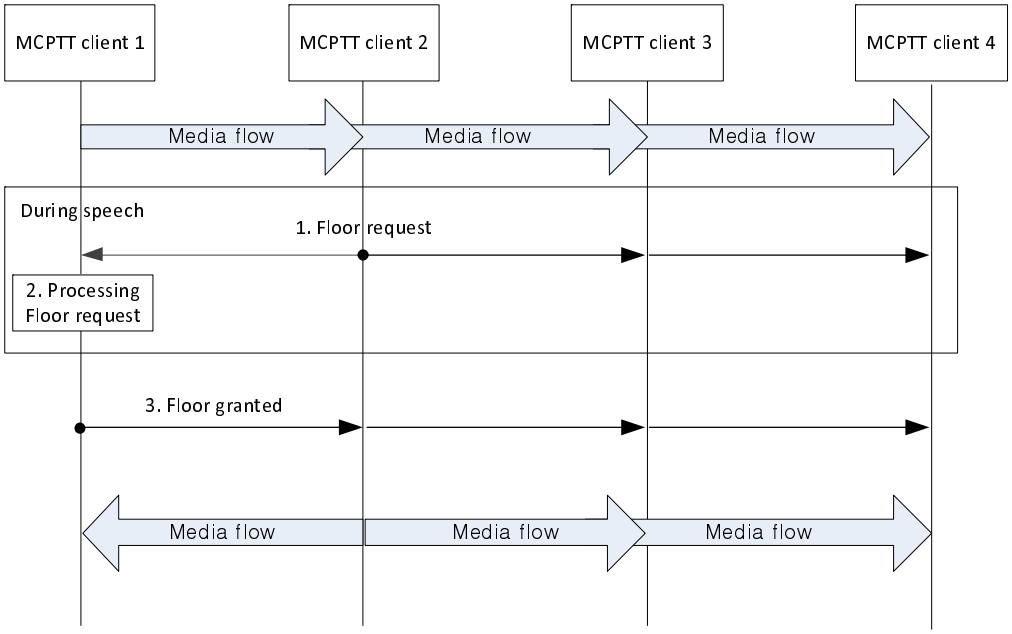

Figure 10.9.2.7-1: Floor request with override authorization

1. MCPTT client 2 sends the floor request message with override criteria (e.g., priority level) to the MCPTT group.
2. MCPTT client 1 acting as the floor arbitrator determines if the floor is to be revoked based on override criteria. If this is the case, MCPTT client 1 revokes its right of the floor and stops sending the voice media immediately.
3. MCPTT client 1 sends the floor granted message to the MCPTT group. The floor granted message contains the MCPTT ID to be granted, the floor and the floor control queue (if supported). MCPTT client 1 may also include the maximum duration that MCPTT client 2 can transmit voice in the floor granted message.

MCPTT client2 who has revoked the floor is the new floor arbitrator and transmits the audio media to the MCPTT group.

10.9.2.8 Floor queue status

Figure 10.9.2.8-1 shows the high level procedure that the floor control is conducted when the MCPTT off-network session is already established among MCPTT floor participants and while voice media is transmitting. If the floor control queueing is supported by the floor control mechanism, the current speaking MCPTT group member who is acting as the floor arbitrator collects the information about the queue status based on the received request(s) from the MCPTT group participant(s). The current speaker can then share information about the queue status of the MCPTT floor participant upon request.

NOTE: The description only applies to group calls.

Pre-condition:

- MCPTT client 1, who acts as the floor arbitrator, transmits the audio media to the MCPTT group.

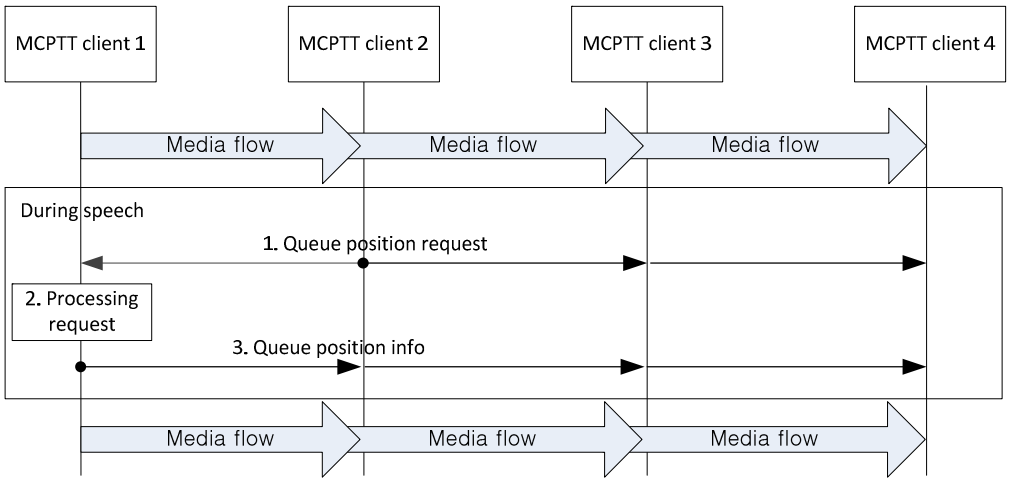

Figure 10.9.2.8-1: Queue status request

1. MCPTT client 2 sends the queue position request message targeted to MCPTT client 1 i.e. the floor arbitrator by broadcasting the message to the MCPTT group to get its queue status.
2. Since the queue function is assumed to be supported in this call flow, MCPTT client 1 i.e. the floor arbitrator processes the queue position request to find out the status of MCPTT client 1 in the queue.
3. MCPTT client 1 constructs the queue position info message containing the MCPTT client 2's queue status and sends it toward MCPTT client 2 by broadcasting the message to the MCPTT group.

MCPTT client1 continues being the floor arbitrator and transmits the audio media to the MCPTT group.

10.10 Use of MBMS transmission

10.10.1 Information flows for MBMS Transmission

10.10.1.1 MBMS bearer announcement

Table 10.10.1.1-1 describes the information flow MBMS bearer announcement from the MCPTT server to the MCPTT client.

Table 10.10.1.1-1: MBMS bearer announcement

Information element	Status	Description
TMGI	M	TMGI information
QCI	M	QCI information used by the ProSe UE-Network Relay to determine the ProSe Per-Packet Priority value to be applied for the multicast packets relayed to Remote UE over PC5
Source IP address	M	The source address of the content delivered over the MBMS bearer
List of service area identifier	M	A list of service area identifier for the applicable MBMS broadcast area.
Frequency	O	Identification of frequency in case of multi carrier support
IP Multicast address	M	IP Multicast address of MBMS bearer
Destination port	M	Multicast destination UDP ports used on the MBMS bearer
SDP	M	SDP with media information sent by server (e.g. codec, protocol id)

10.10.1.2 Call connect and disconnect over MBMS

Table 10.10.1.2-1 describes the information flow to associate a MCPTT group call to a MBMS bearer. It is sent from the MCPTT server to the MCPTT client.

Table 10.10.1.2-1: MapGroupToBearer

Information element	Status	Description
MCPTT group ID	M	This element identifies the MCPTT group, in which the call is started.
Media stream identifier	M	This element identifies the media stream in the SDP used for the group call (e.g. an identifier of the m= line in the SDP).
TMGI	O	The MBMS bearer identifier if the MCPTT group call is not sent on the same MBMS bearer as this connect message.

Table 10.10.1.2-2 describes the information flow to disconnect a MCPTT group call from a MBMS bearer. It is sent from the MCPTT server to the MCPTT client.

Table 10.10.1.2-2: UnmapGroupFromBearer

Information element	Status	Description
MCPTT group ID	M	This element identifies the MCPTT group, in which the call is started.

10.10.2 Use of pre-established MBMS bearers

10.10.2.1 GeneralIn this scenario, the MCPTT server pre-establishes MBMS bearer(s) in certain pre-configured areas before the initiation of the group communication session. When a UE originates a request for group call for one of these areas, the pre-established MBMS bearer(s) is used for the DL media transmission.

The following steps needs to be performed prior the start of the MCPTT group call over pre-established MBMS bearer:

- MBMS bearer(s) is Pre-established
- Perform the announcement of the information of pre-established MBMS bearer to the MCPTT clients

When these preparation steps have been done the MCPTT group call using MBMS bearer can start. Both pre-arranged group calls and chat group calls can use the pre-established MBMS bearer for distributing the media.

Both the media packets as well as the floor control messages to the receiving users are sent on the MBMS bearer. Optionally a separate MBMS bearer could be used for the floor control messages, due to different bearer characteristic requirements.

10.10.2.2 Procedure

The procedure figure 10.10.2.2-1 shows only one of the receiving users using MBMS bearer. There might also be users in the same MCPTT group call that receives the call on unicast bearer.

Pre-conditions:

- The participating users are already affiliated.

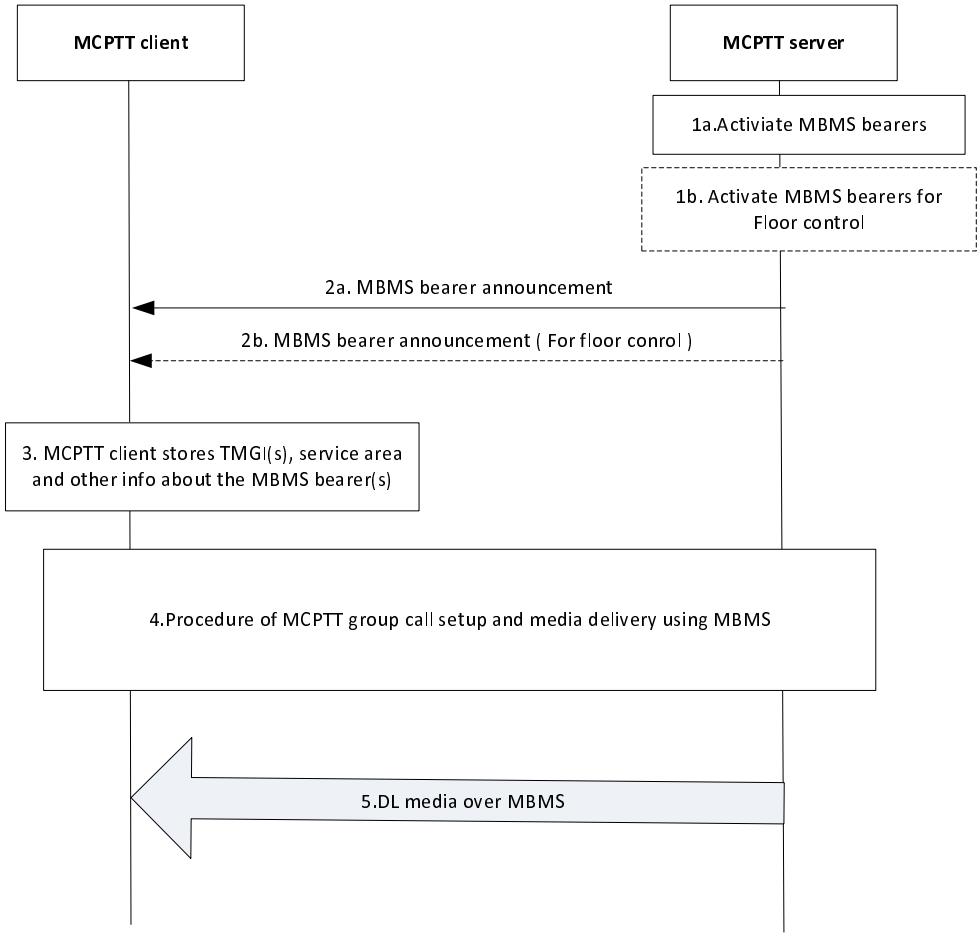

Figure 10.10.2.2-1: Use of pre-established MBMS bearers

1a. The MCPTT server determines to activate MBMS bearer. The activation of the MBMS bearer is done on MB2-C reference point and according to 3GPP TS 23.468 [10]. The activation message should include TMGI, QoS, MBMS broadcast area, start time. This bearer will be used for the MCPTT media.

1b. optionally, the MCPTT server may also activate a MBMS bearer dedicated for floor control signalling. The activation of the MBMS bearer is done on MB2-C reference point and according to 3GPP TS 23.468 [10]. The activation message should include TMGI, QoS, MBMS broadcast area, start time. This bearer will be used for the MCPTT floor control signaling.

NOTE 1: The procedure to determine the activation of MBMS bearers is implementation specific.

2a. The MCPTT server passes the MBMS service description associated with the pre-established MBMS bearer to the MCPTT UE. The MCPTT client obtains the TMGI, identifying the MBMS bearer, from the service description.

2b. The MCPTT server may pass the MBMS service description associated with the pre-established floor control MBMS bearer to the MCPTT client. The MCPTT client obtains the TMGI, identifying the MBMS bearer, from the service description.

NOTE 2: Step 2a and Step 2b can be done in one MBMS bearer announcement message.

3. The MCPTT client stores the information associated with the TMGI(s).

4. An MCPTT group call is established. When MCPTT server decide to use the MBMS bearer for media transmission for this MCPTT group call, the procedure of call connect and disconnect over MBMS as defined in subclause 10.10.4 is triggered.

5a. The MCPTT client uses the TMGI and other MBMS bearer related information to activate the monitoring of the MBMS bearer by the MCPTT UE.

5b. The MCPTT server transmits the media over the MBMS bearer.

5c. Media packets are detected and delivered to the MCPTT client.

10.10.3 Use of dynamic MBMS bearer establishment

In this scenario depicted in figure 10.10.3-1, the MCPTT server uses a unicast bearer for communication with the UE on the DL at the start of the group communication session. When the MCPTT server decides to use an MBMS bearer for the DL media transmission, the MCPTT server establishes an MBMS bearer using the procedures defined in 3GPP TS 23.468 [10]. The MCPTT server provides the MBMS service description associated with MBMS bearer(s), obtained from the BM-SC, to the UE. The UE starts using the MBMS bearer(s) to receive DL media and stops using the unicast bearer for the DL media transmission.

NOTE 1: The MCPTT server logic for determining when to establish the new MBMS delivery bearer is implementation specific. For example, the MCPTT server could decide to establish the MBMS delivery based on the location of the UE's that are a part of the group communication session.

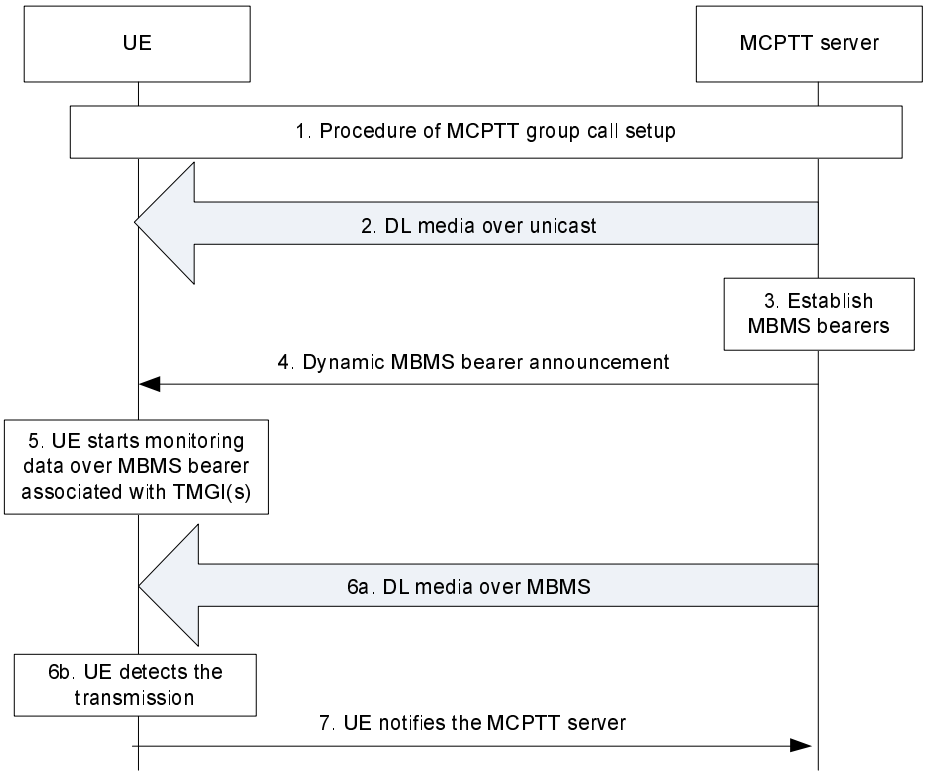

Figure 10.10.3-1: Use of dynamic MBMS bearer establishment

1. An MCPTT group call is established.

NOTE 2: The MCPTT group call can be any types established by any procedure in subclause 10.6.2.1.

2. The downlink data is sent by unicast delivery.
3. The MCPTT server establishes the MBMS bearer(s) for the group communication session according to the procedures defined in 3GPP TS 23.468 [10]. Service description associated with the MBMS bearer(s) is returned from The BM-SC.
4. The MCPTT server provides the service description associated with the MBMS bearer to the UE. The UE obtains the TMGI from the service description.
5. The MCPTT UE starts monitoring data over MBMS associated with the TMGI.
6. The UE detects the transmission corresponding to the TMGI.
7. The MCPTT UE notifies the MCPTT server.

10.10.4 Call connect and disconnect over MBMS

10.10.4.1 General

MBMS bearer can be used for MCPTT group calls. One MBMS bearer is not associated to one specific group or group call. Before sending media packets of a group call over MBMS bearer, the MCPTT server shall send the association information between group call and the MBMS bearer. The group call setup procedure indicates the media stream within one MBMS bearer that is used for the specific group call. When the group call over the MBMS bearer is finished, this temporary association information of an MCPTT group call to specific resources on a MBMS bearer is undone. The procedure in figure 10.10.4.2-1 requires that the group session is setup before the call start. This eliminates the need for the receiving clients to continuously use a unicast bearer. Furthermore the MBMS bearer shall be activated and announced to the MCPTT clients.

10.10.4.2 Procedure

In figure 10.10.4.2-1 the MCPTT client 1 is the client that initiate an MCPTT chat group call and also the transmitting client. MCPTT client 1 may, but does not have to be in an MBMS service area. The MCPTT client 2 and MCPTT client 3 represents MCPTT clients receiving the MCPTT call over an MBMS bearer. There may be other receiving clients both over unicast bearers and over this or other MBMS bearer(s), however they are not illustrated in this figure.

The same procedure as for chat group call can also be applied for pre-arranged calls. However that requires that the pre-arranged sessions are already active. If a pre-arranged group session is initiated the use of pre-established sessions are required.

Editor's note: It is FFS if pre-arranged call using MBMS can be supported without the use of pre-established session.

Pre-conditions:

- All users participating in the MCPTT group call are already affiliated to the group.
- All participating users have joined the group session.

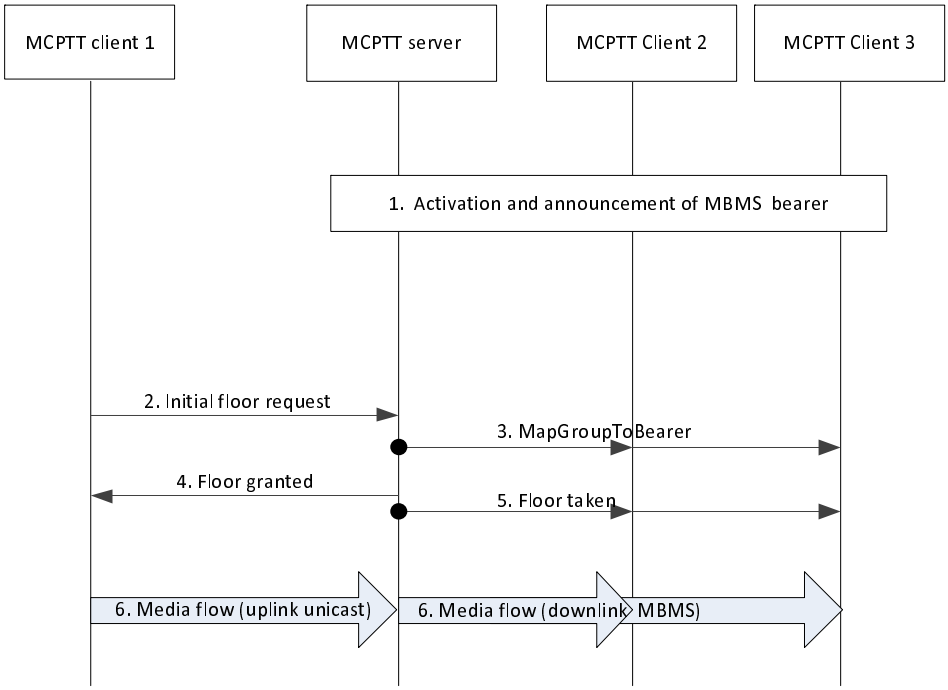

Figure 10.10.4.2-1: Chat group call connect on MBMS bearer

1. Activation and announcement of MBMS bearer availability.

NOTE 1: The procedure does not include the steps for MCPTT client location reporting, or for MBMS capability information exchange.

2. MCPTT client 1 initiate the MCPTT group call by sending an initial floor request over a unicast bearer to the MCPTT server (reference point MCPTT-4).

3. The MCPTT server will send a MapGroupToBearer message over a previously activated MBMS bearer to all users that will receive the call over an MBMS bearer. The MapGroupToBearer message includes association information between the group call and MBMS bearer. The MapGroupToBearer message includes MCPTT group ID and an identifier of the media stream in the activated MBMS bearer and may include the identifier (i.e. the TMGI) of the MBMS bearer broadcasting the call.. The message is sent over reference point MCPTT-9.

NOTE 2: Step 3 can be deferred until step 5 and the MapGroupToBearer message can then be included in the floor taken message.

4. The MCPTT server grants the right to transmit for MCPTT client 1 and by that sends a floor grant message to the MCPTT client 1. This message is sent over a unicast bearer (reference point MCPTT-4).

5. A floor taken message is sent from the MCPTT server to all receiving users. This message includes the MCPTT ID of the transmitting MCPTT client as well as the MCPTT group ID. The message is sent over a MBMS bearer to all users that have previously been setup to receive calls over the MBMS bearer. The message is sent over reference point MCPTT-9.

6. The media is sent from MCPTT client 1 to the MCPTT server over unicast and from the MCPTT server to the MCPTT client 2 and MCPTT client 3 over MBMS bearer.

NOTE 3: Additional floor request messages in the same call will not trigger the MapGroupToBearer message to be sent.

Figure 10.10.4.2-2 shows the high level procedure where a UnmapGroupFromBearer message is sent by the MCPTT server to the MCPTT clients to indicate that the MCPTT group call is being dissociated from the MBMS bearer.

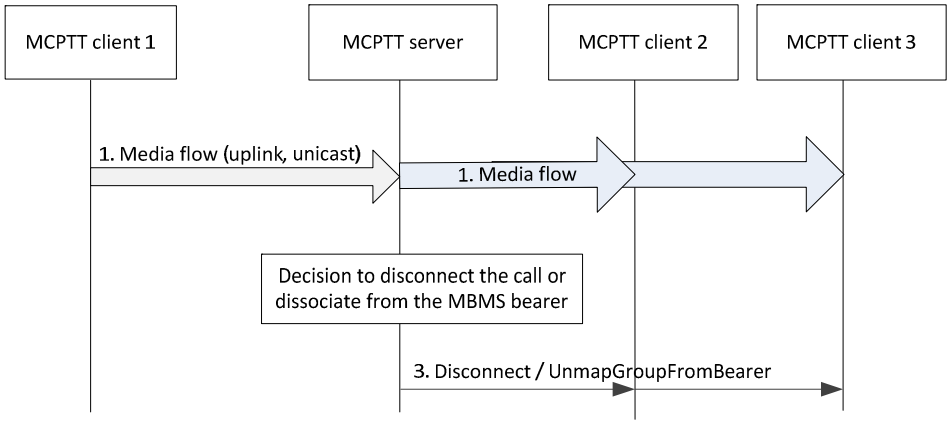

Figure 10.10.4.2-2: Chat group call disconnect on MBMS bearer

1. An MCPTT group call is ongoing; the media is broadcasted over MBMS bearer to MCPTT client 2 and MCPTT client 3.
2. MCPTT server has determined to disconnect the call over the MBMS bearer for the MCPTT clients
3. An UnmapGroupFromBearer message is sent by the MCPTT server to MCPTT client 2, MCPTT client 3 and possibly to MCPTT client 1 (if in MBMS coverage area) on MBMS bearer(s).

NOTE 4: The UnmapGroupFromBearer message can be sent as part of other messages.

NOTE 5: The UnmapGroupFromBearer message and the MapGroupToBearer message can be combined, to facilitate switching bearers in one signalling step, as necessary.

10.11 MCPTT resource management

10.11.1 General

The MCPTT server setup media bearers and may need to modify the bearers for an already established MCPTT call or session (pre-established session or chat group session). The MCPTT server may need to modify unicast media bearers and/or multicast media bearers.

Media characteristics that may need to be modified include:

- activation and deactivation of the bearer;
- modification of the QoS characteristics of the bearer (e.g. bearer priority adjustment); and
- modification of GBR due to media codec change

NOTE: A group call can consist of both unicast and multicast bearers which can all need modification due to the same event.

10.11.2 Request for unicast resources at session establishment

The procedure defined in this subclause specifies how network resources are requested at session establishment. If concurrent sessions are used the MCPTT server may utilize the capability of resource sharing specified in 3GPP TS 23.203 [4]. Specifically the uplink bandwidth can be shared between most types of MCPTT call. The request for resources is sent to the PCRF on the Rx reference point and includes media type, bandwidth, priority and resource sharing information.

The procedure is generic to any type of session establishment that requires requests for network resources.

Procedures in figure 10.11.2-1 are the signalling procedures for the requesting resource at session establishment.

Pre-Conditions:

- No EPS bearer is active with the same QCI/ARP combination
- Normal call setup procedures applies

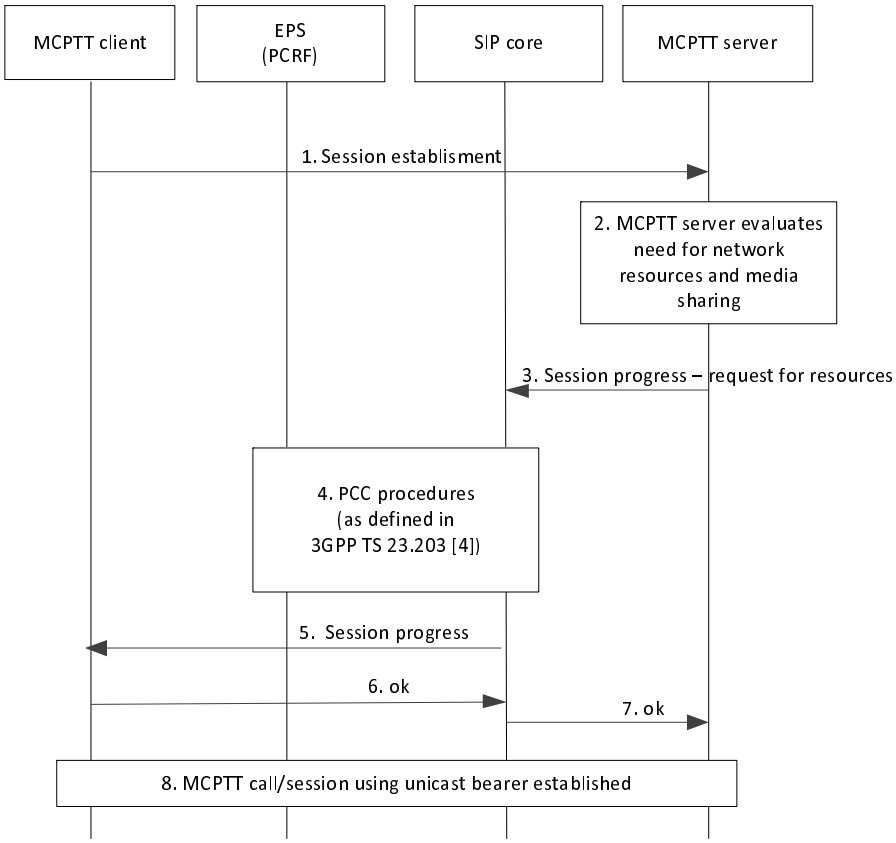

Figure 10.11.2-1: Resource request at session establishment

1. MCPTT client sends a call/session establishment request.
2. MCPTT server receives evaluates the need network resources and use of media resource sharing.
3. MCPTT server send a session progress request containing request for resources. .
4. PCC procedures (as defined in 3GPP TS 23.203 [4]) initiated from SIP core local inbound/outbound proxy over Rx.
5. The SIP core local inbound / outbound proxy forwards the call control protocol request to the MCPTT client.
6. The MCPTT client acknowledges the session progress request with an OK message.
7. The SIP core local inbound / outbound proxy forwards the OK message to the MCPTT server.
8. The MCPTT call/session is established and resources have been allocated.

10.11.3 Request for modification of unicast resources

To modify unicast media bearers the MCPTT server shall send a bearer modification request containing the parameters to be modified (active/inactive, priority/QoS, codec) using the call control protocol via the SIP core to the UE.

The following procedure focuses on the case where the MCPTT server is upgrading an existing MCPTT call to an MCPTT emergency or imminent threat call while the MCPTT call is already in progress.

Procedures in figure 10.11.3-1 are the signalling procedures for the modification of a unicast bearer when the MCPTT server is upgrading an existing MCPTT call to an MCPTT emergency or imminent threat call while the MCPTT call is already in progress:

Pre-conditions:

- An MCPTT call is already in progress;
- A unicast bearer is being used for the call;
- A request has been made to upgrade the call to an MCPTT emergency or imminent threat call.

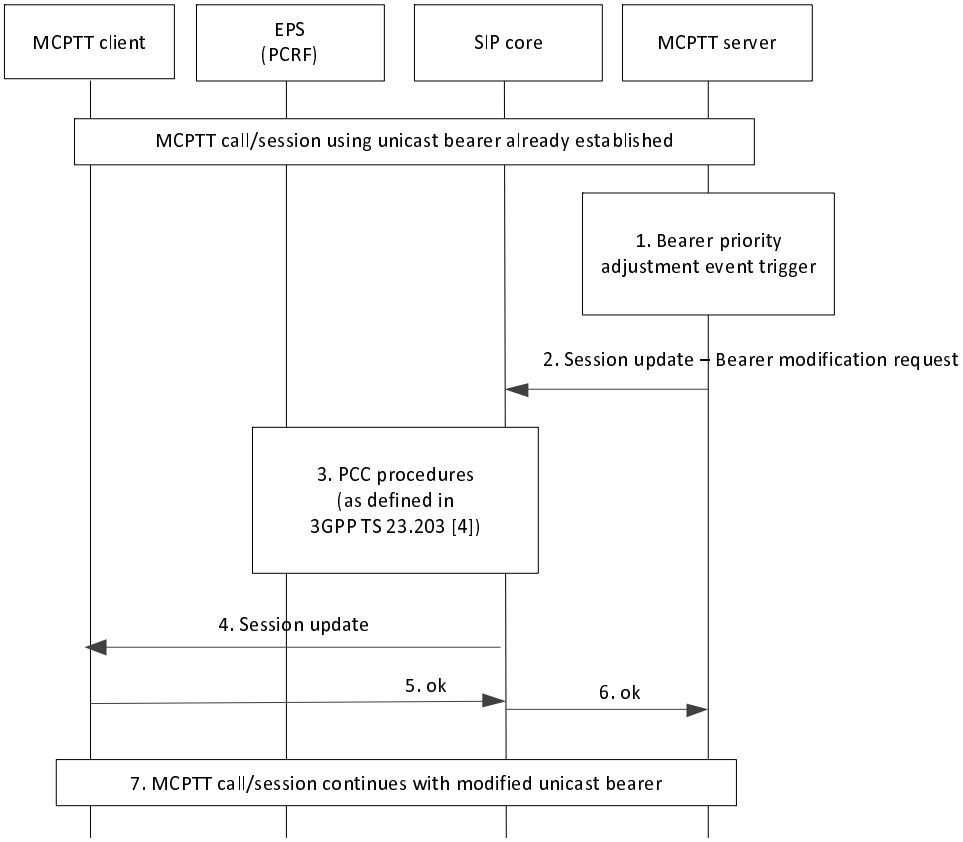

Figure 10.11.3-1: Bearer modification request

1. MCPTT server receives an event that triggers the need to modify the priority of a unicast bearer (.e.g. a request to upgrade the existing MCPTT call to an MCPTT emergency or imminent threat call).
2. MCPTT server sends a session update request containing an indication of the new priority of the unicast bearer.
3. PCC procedures (as defined in 3GPP TS 23.203 [4]) initiated from SIP core local inbound/outbound proxy over Rx.
4. The SIP core local inbound / outbound proxy forwards the session update request to the MCPTT client.
5. The MCPTT client acknowledges the call control protocol request with an OK message.
6. The SIP core local inbound / outbound proxy forwards the OK message to the MCPTT server.
7. The MCPTT call continues with the modified unicast bearer.

10.11.4 Management of multicast media bearers

To activate the multicast media bearers the MCPTT server shall use the Activate MBMS Bearer procedure specified in 3GPP TS 23.468 [10] with the MCPTT server performing the GCS AS function.

To deactivate the multicast media bearers the MCPTT server shall use the Deactivate MBMS Bearer procedure specified in 3GPP TS 23.468 [10] with the MCPTT server performing the GCS AS function.

To modify multicast media bearers the MCPTT server shall use the Modify MBMS Bearer procedure specified in 3GPP TS 23.468 [10] with the MCPTT server performing the GCS AS function.

10.11.5 Request for resources with shared priority

10.11.5.1 General

An MCPTT server that supports simultaneous sessions may need to share a common priority on the EPS bearer for several MCPTT group calls that may use different priorities on the application level. This is achieved by including information for priority sharing on the request of resources over Rx reference point to PCRF. All sessions associated with the same priority sharing information will be handled by one EPS bearer, which will have a priority based on the highest requested priority among the sessions.

The use of the procedure defined in subclause 10.11.5.2 is dependent on operator policy.

10.11.5.2 Procedure

Pre-conditions:

- All previous resource requests from the MCPTT have included a priority sharing information.

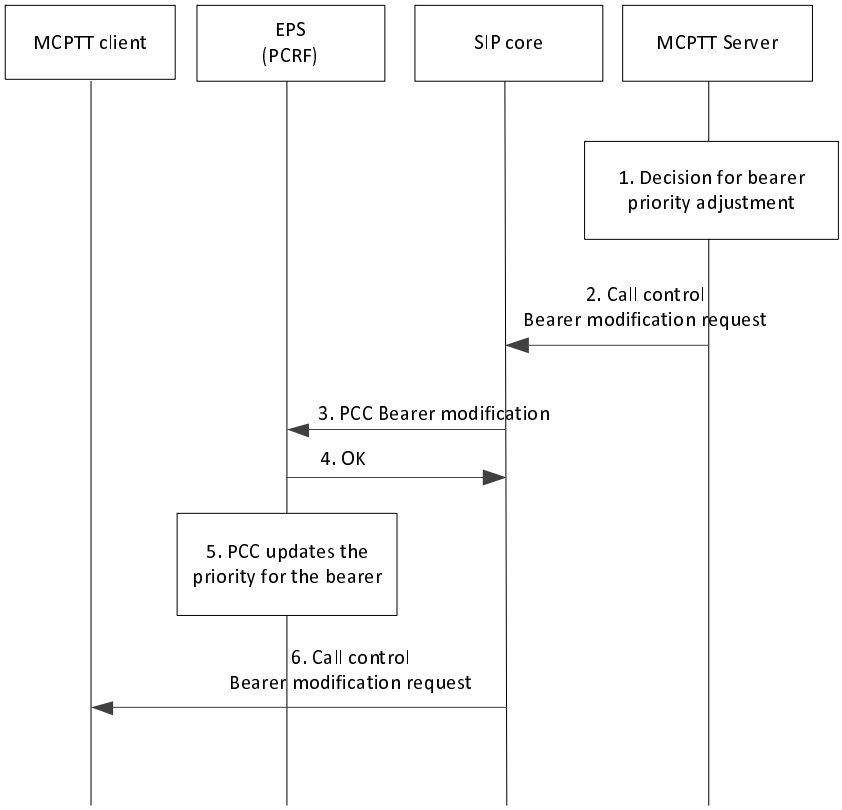

Figure 10.11.5.2-1: Resource request including priority sharing information

1. The MCPTT server decides based on a request from the MCPTT client that the priority of an ongoing call must be adjusted. An example of this is when an MCPTT group call is changed to an emergency call (see subclause 10.6.2.6.1.2).

2. The MCPTT server requests a session update to the SIP core. This request will contain information of priority sharing.

3. The proxy function in the SIP core sends a request to the PCRF over Rx to request for modified priority. The request will include the priority sharing information over Rx.

4. The PCRF acknowledges the request.

5. PCC updates the bearer priority for the bearer that contains the SDFs associated with the same priority sharing information. The priority is set to highest priority (lowest ARP) among those SDFs. No additional bearer is created. Also the default bearer priority is updated accordingly.

6. The session update is forwarded to the MCPTT client.

NOTE 1: The procedure defined above requires a PCC enhancement and is subject to implementation in EPC and IMS and can therefore only be used if supported by EPC and IMS.

NOTE 2: If the EPC and IMS does not support the priority sharing from MCPTT system, no shared priority treatment apply, and a new EPS bearer will be setup based on QCI/ARP combination.

10.12 MCPTT media plane transmissions with partner MCPTT systems

The MCPTT user is able to receive MCPTT media services (group communication, private calls, etc) from partner MCPTT systems in normal and roaming conditions. In this service delivery model, the media plane transmissions between the MCPTT UE of the user and the partner MCPTT system can be achieved directly or via the primary MCPTT system, selected by the PLMN operator's policy. The protocol used for media plane signalling is non-SIP like RTCP.

Figure 10.12-1 and figure 10.12-2 provide the procedures for media related signalling and the media transmission between MCPTT UE of the user and the partner MCPTT system.

Pre-conditions:

1. The MCPTT group is defined in the partner MCPTT system, where the MCPTT client of user receives the MCPTT service.

2. An MCPTT group call is set up and active.

3. The partner MCPTT system is the group host MCPTT server that is hosting the MCPTT group. The corresponding floor control server manages the media corresponding to the group call.

4. Protocol used for signalling of media plane is non-SIP, it can be protocol like RTCP.

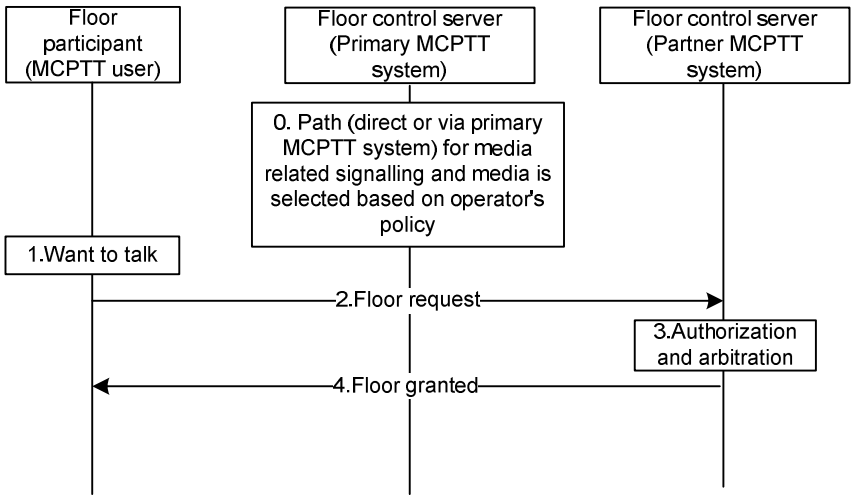

Figure 10.12-1: Media related signalling communication

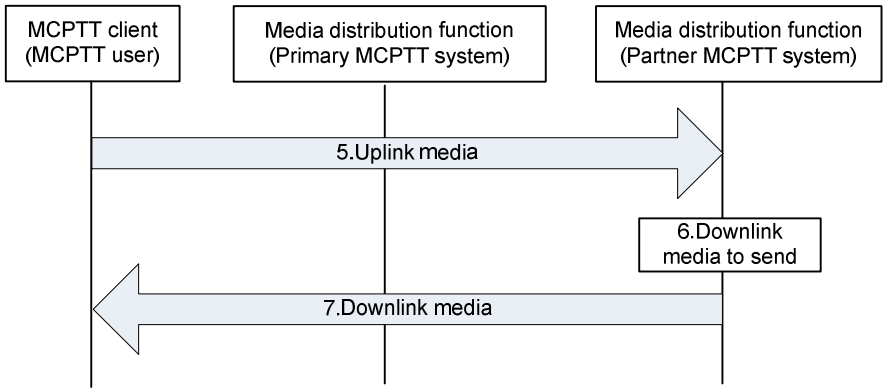

Figure 10.12-2: Media communication

0. Path (direct or via primary MCPTT system) for media related signalling and media between MCPTT UE and partner MCPTT system is selected based on PLMN operator's policy.

For media related signalling communication:

1. An MCPTT user wants to talk.
2. The floor participant corresponding to the MCPTT user sends a floor request message to floor control server (partner MCPTT system) to get the authorization and/or permission to talk.
3. The floor control server (partner MCPTT system) performs the authorization and arbitrates between requests that are in contention (i.e., floor control).
4. If the floor control server (partner MCPTT system) allows the floor participant to talk, a floor granted is provided with permission granted to talk.

For media communication:

5. The MCPTT client can now send uplink media data to the media distribution function of the MCPTT server (partner MCPTT system).
6. The media distribution function of the MCPTT server (partner MCPTT system) has downlink media data to transfer.
7. The media distribution function of the MCPTT server (partner MCPTT system) transfers the downlink media to the MCPTT client of the MCPTT user.

10.13 Use of UE-to-network relay

10.13.1 UE-to-network relay service authorization

The MCPTT service shall support the capability for UE-to-network relay to restrict the relayed group communication on a per group basis.

To meet the above requirement, ProSe (as specified in 3GPP TS 23.303 [8]) can be used with an appropriate relay service code as per the following:

- To restrict connection from only the membership of allowed MCPTT groups, UE-to-network relay UE is provisioned with relay service code(s) associated with allowed MCPTT group(s). The UE-to-network relay performs the access control as follows:

  1) The UE broadcasts which MCPTT group(s) is/are authorized to connect to the network over this UE-to-network relay by including the related relay service code(s) in the UE-to-Network Relay Discovery Announcement message (as specified in 3GPP TS 23.303 [8]); or

2) The UE determines whether to respond to a remote UE"s broadcasting message by checking if the relay service code carried in the UE-to-Network Relay Discovery Solicitation message is within the list of allowed relay service codes.

- To find a permitted UE-to-network relay, a remote UE is provisioned with the relay service code(s) associated MCPTT group(s) which the MCPTT user belongs to. The remote UE performs the UE-to-network relay selection as follows:

1) The remote UE determines if it is allowed to connect to a particular UE-to-network relay by checking whether the relay service code(s) associated with its MCPTT group(s) is/are carried in UE-to-Network Relay Discovery Announcement message (as specified in 3GPP TS 23.303 [8]; or

2) The remote UE includes the relay service code(s) associated with its MCPTT group(s) in Network Relay Discovery Solicitation message (as specified in 3GPP TS 23.303 [8]).

10.13.2 UE-to-network relay MCPTT service

The ProSe UE-to-network relay provides a purely layer 3 IP data routing service, when the remote UE loses the coverage of cellular network and the MCPTT user on the remote UE requires to access the MCPTT service via a ProSe UE-to-network relay.

The application layer signalling for the MCPTT user on a remote UE are identical to the application layer signalling for the MCPTT user on an on network UE.

10.14 Location information

10.14.1 General

MCPTT client location information shall be provided by the MCPTT client to the MCPTT server. The location information reporting triggers are based on the location configuration. Different type of location information can be provided.

10.14.2 Information flows for location information

10.14.2.1 Location reporting configuration

Table 10.14.2.1-1 describes the information flow from the MCPTT server to the MCPTT client for the location reporting configuration.

Table 10.14.2.1-1: Location reporting configuration

Information element	Status	Description
Requested non-emergency location information	O (NOTE)	Identifies what location information is requested, except for MCPTT emergency or imminent peril calls or MCPTT emergency alerts
Requested emergency location information	O (NOTE)	Identifies what location information is requested, for MCPTT emergency or imminent peril calls or MCPTT emergency alerts
Triggering criteria in non-emergency cases	O (NOTE)	Identifies when the MCPTT client will send the location report in non-emergency cases
Minimum time between consecutive reports	O (NOTE)	Defaults to 0 if absent. or in case of MCPTT emergency or imminent peril calls or MCPTT emergency alerts
NOTE: At least one of these rows shall be present.		

10.14.2.2 Location information report

Table 10.14.2.2-1 describes the information flow from the MCPTT client to the MCPTT server for the location information reporting.

Table 10.14.2.2-1: Location information report

Information element	Status	Description
MCPTT ID	M	Identity of the reporting client
Triggering event	M	Identity of the event that triggered the sending of the report
Location Information	M	Location information

10.14.2.3 Location information request

Table 10.14.2.3-1 describes the information flow from the MCPTT server to the MCPTT client for requesting an immediate location information report.

Table 10.14.2.3-1: Location information request

Information element	Status	Description
MCPTT ID	M	Identity of the reporting client

10.14.2.4 Event-triggered location reporting procedure

The MCPTT server provides location reporting configuration to the MCPTT clients, indicating what information the MCPTT server expects and what events will trigger the sending of this information to the MCPTT server. The decision to report location information can be triggered at the MCPTT client by different conditions, e.g., the reception of the location reporting configuration, initial registration, distance travelled, elapsed time, cell change, SAI change, tracking area change, PLMN change, MCPTT call initiation, or other types of events such as MCPTT emergency alert, MCPTT emergency call or MCPTT imminent peril calls. The location report can include information described in subclause 7.5.2.2 and other location information.

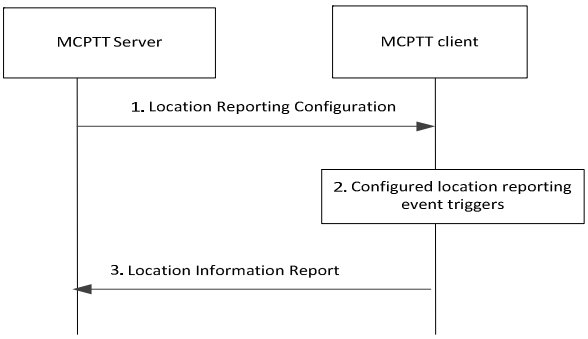

Figure 10.14.2.4-1: Event-triggered location reporting procedure

1. The MCPTT server sends location reporting configuration to the MCPTT client containing the initial configuration (or a subsequent update) for reporting the location of the MCPTT UE.

NOTE 1: The location reporting configuration information can be made part of the MCPTT user profile, in which case the sending of the message is not necessary.

NOTE 2: Different MCPTT clients may be given different location reporting criteria.

2. A location reporting event occurs, triggering step 3.

3. The MCPTT client sends a location information report to the MCPTT server, containing location information identified by the MCPTT server and available to the MCPTT client.

10.14.2.5 On-demand location reporting procedure

The MCPTT server provides location reporting configuration to the MCPTT clients, indicating what information the MCPTT server expects. Subsequently, the MCPTT server can request a location report at any time by sending a location information request, which will cause the client to immediately send the location report. The location report can include information described in subclause 7.5.2.2 and other location information.

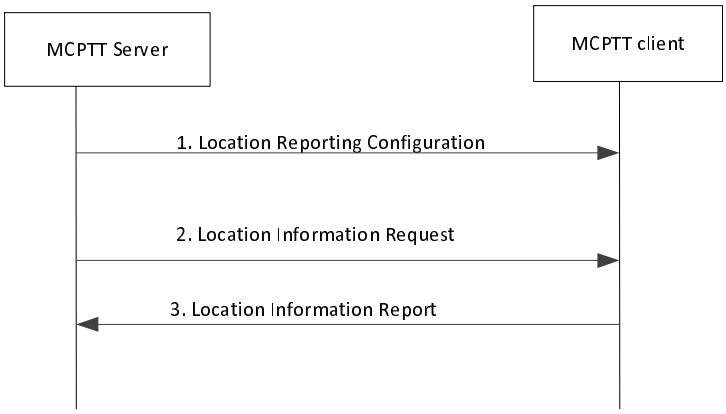

Figure 10.14.2.5-1: On-demand location information reporting procedure

1. The MCPTT server sends location reporting configuration to the MCPTT client containing the initial configuration (or a subsequent update) for reporting the location of the MCPTT UE.

NOTE 1: The location reporting configuration information may be made part of the MCPTT user profile, in which case the sending of the message may not be necessary.

NOTE 2: Different MCPTT clients may be given different location reporting criteria.

2. The MCPTT server sends a location information request.

3. The MCPTT client immediately responds to the MCPTT server with a report containing location information identified by the MCPTT server and available to the MCPTT client.

Annex A (informative): Service continuity for MCPTT

A.1 Service continuity between on-network MCPTT service and UE-to-network relay MCPTT service

This annex describes how 3GPP TS 23.237 [6] mechanisms for IMS service continuity can be used to provide service continuity between on-network MCPTT service and UE-to-network relay MCPTT service.

Only the procedure for service continuity from on-network MCPTT service to UE-to-network relay MCPTT service is described in figure A.1-1. The procedure for service continuity in the opposite direction is identical.

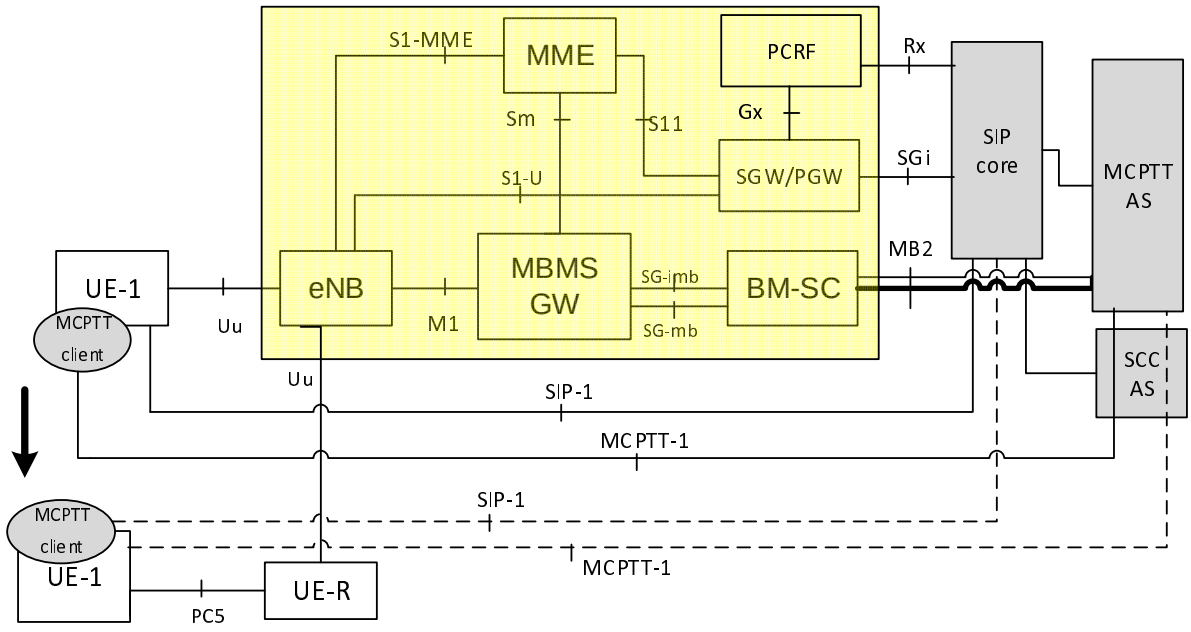

Figure A.1-1: Service continuity from on-network to UE-to-network relay

As illustrated in figure A.1-1:

- Initially UE-1 has a direct connection to the network (on-network MCPTT service). It is registered with the SIP core and is engaged in a SIP session with the MCPTT Application Server (solid lines SIP-1 and MCPTT-1 in figure A.1-1).
- When UE-1 realises that it is losing connection to the network, or after the connection to the network has been lost, UE-1 discovers a UE-to-network relay (UE-R) and establishes a PC5 connection with UE-R. UE-1 registers with the SIP core over the target access leg and enters UE-to-network relay MCPTT service by transferring the media streams over the target leg (dashed lines SIP-1 and MCPTT-1 in figure A.1-1).
- The SIP session is anchored at a Service Centralisation and Continuity Application Server (SCC AS) before and after the handover, as described in 3GPP TS 23.237 [6].

Depicted in figure A.1-2 is the call flow for service continuity when the UE switches from on-network MCPTT service to UE-to-network MCPTT relay service.

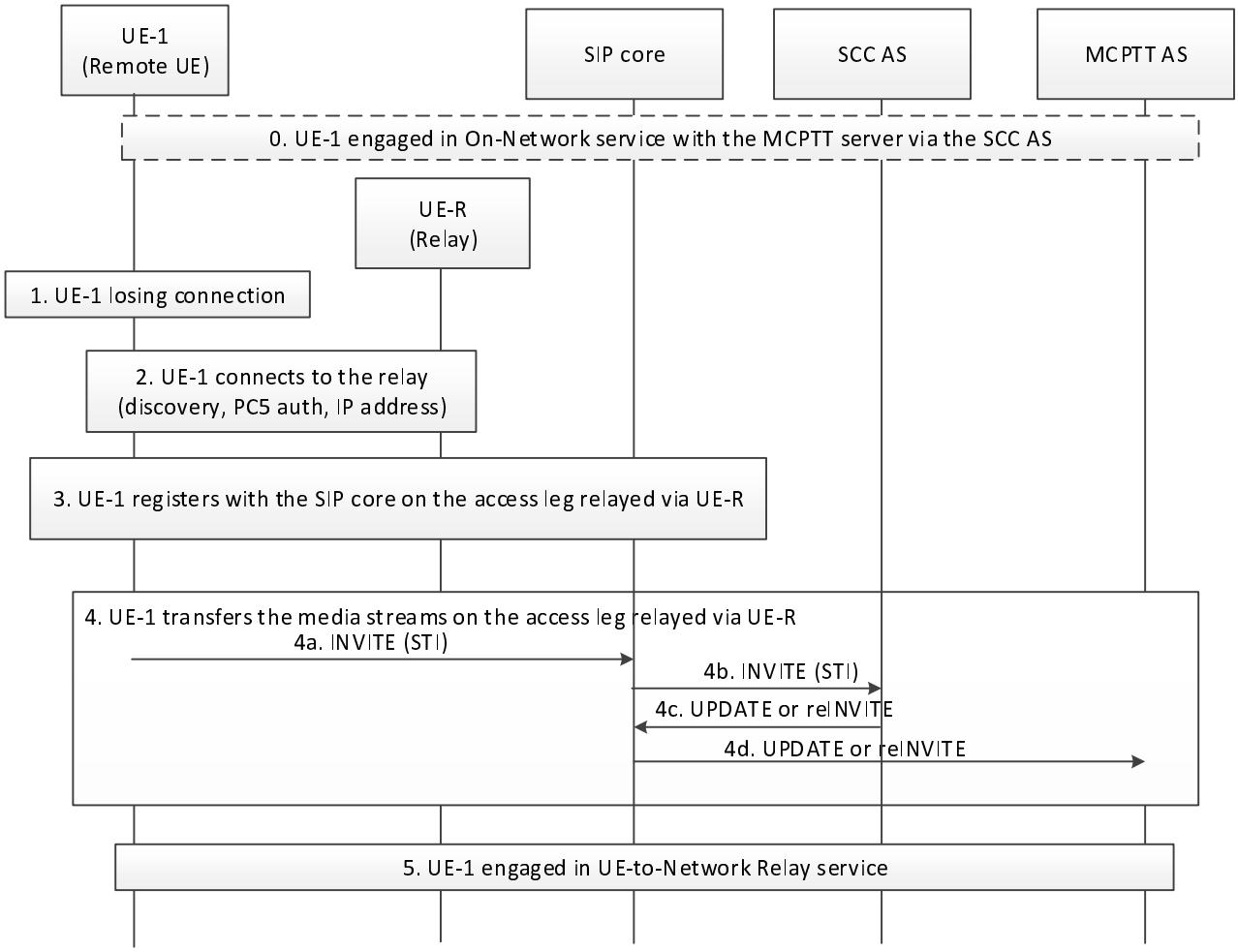

Figure A.1-2 Service continuity when UE switches from on-network MCPTT service to UE-to-network relay MCPTT service

0. UE-1 has a direct connection to the network and is engaged in a SIP session with the MCPTT AS (on-network MCPTT service). The SIP session is anchored at a Service Centralisation and Continuity Application Server (SCC AS) and a Session transfer Identifier (STI) is assigned for the anchored SIP session, as described in 3GPP TS 23.237 [6].

1. UE-1 realises that it is losing connection to the network or has completely lost it.

2. UE-1 (in the role of remote UE) performs ProSe UE-to-network relay discovery over PC5 and establishes a secure point-to-point link with the relay (UE-R) over PC5. As part of this process the remote UE is mutually authenticated at PC5 layer with either the relay or with the network as specified in 3GPP TS 23.303 [8]. In the process UE-1 is also assigned an IP address/prefix by the relay.

NOTE 1: If step 2 is started after losing connection, the service interruption can be noticeable to the user.

NOTE 2: Step 2 will be entirely described under in 3GPP TS 23.303 [8].

3: UE-1 registers with the SIP core over the UE-to-network relay leg.

4. In order to transfer the media streams of the SIP session UE-1 sends an INVITE message on the new access leg towards the SCC AS. The INVITE message includes the STI identifying the session to be transferred. The SCC AS identifies the session based on STI and updates the session over the remote access leg i.e. towards the MCPTT AS.

5. The procedure is completed when all media streams have been transferred on the access leg relayed via UE-R. At this point UE-1 may deregister the on-network leg if it still has direct network connection (not shown in the figure).

NOTE 3: The procedure for service continuity is always completed with unicast delivery on the target side. If MCPTT content is being distributed on the target side in multicast mode, then switching from unicast to multicast delivery is performed after completion of the service continuity procedure.

Annex B (normative): MCPTT related data

B.1 General

This Annex contains tables of configuration data needed for MCPTT. Configuration data belongs to one of the following categories:

- UE configuration data, as specified in subclause B.2;
- User configuration data, as specified in subclause B.3;
- Group configuration data, as specified in subclause B.4;
- Service configuration data, as specified in subclause B.5; and
- Initial configuration data, as specified in subclause B.6.

Additionally, initial configuration data needed to access the MCPTT service is specified in subclause B.6.

For each of data item, a reference to the introduction requirements from 3GPP TS 22.179 [2] or a reference to the related subclause from the present document is given.

For each configuration category, data is split between configuration data that is applicable to both on-network and off-network, configuration data that is applicable to on-network only, and configuration data that is applicable to off-network only. The data in each configuration category corresponds to a single instance of the category type, this means that the UE, Group, User and Service configuration data refers to the information that will be stored against each UE, Group, User and Service. This means that the three separate tables (on-network and off-network, on-network only, off-network only) for each configuration category represent the complete set of data for each configuration data category element.

The columns in the tables have the following meanings:

- Reference: the reference of the corresponding requirement in 3GPP TS 22.179 [2] or the corresponding subclause from the present document.
- Parameter description: A short definition of the semantics of the corresponding piece of data.

Each parameter that can be configured online shall only be configured through one online interface. Each parameter that can be configured offline shall only be configured through one offline interface. The most recent configuration data made available to a UE always overwrites previous configuration data, irrespective of whether the configuration data was provided via online or offline mechanism.

B.2 UE configuration data

Data in tables B.2-1, B.2-2 and B.2-3 has to be known by the MCPTT UE after MCPTT authorization. CSC-4 reference point is used for configuration between configuration management server and MCPTT UE when the UE is on-network.

Data in tables B.2-1 and B.2-3 can be configured offline using the CSC-11 interface. Tables B.2-1 and B.2-3 are the UE configuration required to support the use of off-network MCPTT service.

Table B.2-1: UE configuration data (on and off network)

Reference	Parameter description
[R-5.5.2-005]	Maximum number of simultaneous group calls (N4)
[R-5.5.2-006]	Maximum number of transmissions (N5) in a group
[R-5.5.2-007]	Maximum number of private calls(N10)
[R-5.5.2-010]	Requested presentation priority of Group calls

Table B.2-2: UE configuration data (on network)

Reference	Parameter description
Subclause 10.1.3.3	Relay service (Y/N)
Subclause 10.1.3.3	Allowed relayed MCPTT groups
Subclause 10.1.3.3	Relay service code associated with each MCPTT group

Table B.2-3: UE configuration data (off network)

Reference	Parameter description

B.3 User configuration data (MCPTT user profile data)

Data in table B.3-1, B.3-2, B.3-3 has to be known by the MCPTT UE after MCPTT authorization. CSC-4 reference point is used for configuration between configuration management server and MCPTT UE when the UE is on-network.

Data in table B.3-1 and B.3-3 can be configured offline using the CSC-11 interface. Tables B.3-1 and B.3-3 are the UE configuration required to support the use of off-network MCPTT service.

Table B.3-1: User configuration /MCPTT user profile data (on and off network)

Reference	Parameter description
[R-5.8-001] [R-6.9-003]	Authorised to create and delete aliases of an MCPTT User and its associated user profiles.
[R-5.8-002] [R-6.9-003]	Alphanumeric aliases of user
Subclause 8.1.2	MCPTT user identity (MCPTT ID)
[R-5.1.1-005] [R-5.10-001]	Participant type of the user
[R-5.1.5-004]	Limitation of number of affiliations per user (N2)
[R-5.1.8-006] [R-5.3-002] [R-5.10-001] [R-5.18.2-001] [R-5.18.2-002]	User's Mission Critical Organization (i.e. which organization a user belongs to)
[R-5.5.2-008]	Maximum number of simultaneously received group calls (N6)
[R-5.5.2-009]	Maximum number of simultaneous transmissions received in one group call (N7)
[R-5.6.5-004]	Authorised to make a private call
[R-5.6.5-001]	Authorised to make a private call with manual commencement
[R-5.6.5-003]	List of user (s) who can be called in private call.
[R-5.6.5-002]	Authorised to make a private call with automatic commencement
[R-5.6.3-011] [R-6.7.4-010]	Authorisation of user to force automatic answer for a private call
[R-5.6.5-006] [R-6.7.5-002]	Authorised to restrict the provision of a notification of call failure reason for private call
[R-5.7.2.1.1-001]	Authorisation to make an MCPTT emergency group call functionality enabled for user
[R-5.7.2.1.1-001]	Group used on initiation of an MCPTT emergency group call (currently selected/ dedicated)
[R-5.7.2.1.2-005]	Authorisation to cancel an in progress emergency associated with a group
[R-5.7.2.2.1-001]	Authorised to make an Imminent Peril group call
[R-5.7.2.2.1-009]	Group used on initiation of an MCPTT imminent peril group call (currently selected/ dedicated/ default if no group selected)
[R-5.7.2.2.2-002]	Authorised for imminent in- peril cancelation
[R-5.7.2.3.1-001]	Recipient for an emergency private call (Pre-configured/ user locally determined)
[R-5.7.2.3.1-001]	Authorised to make an emergency private call
[R-5.7.2.3.2-001]	Authorised to cancel emergency priority in a private emergency call by an authorized user
[R-5.7.2.4.1-002]	Authorised to activate emergency alert
[R-5.7.2.4.1-004] [R-5.7.2.4.1-008] [R-5.7.2.4.1-012]	Group / user recipient of an emergency alert (Pre-defined group, currently selected group, pre-defined recipient/ user locally defined recipient/ default if no recipient selected)
[R-5.7.2.4.2-002]	Authorisation to cancel an MCPTT emergency alert
[R-5.19-007] [R-6.13.4-002]	User profile status (enabled/disabled)
[R-5.1.7-002]	Priority of the user for initiating/receiving calls
[R-5.2.2-003]	Authorisation to create a group-broadcast group
[R-5.2.2-003]	Authorisation to create a user-broadcast group

Table B.3-2: User configuration data / MCPTT user profile data (on network)

Reference	Parameter description
Subclause 5.2.5	Group user implicitly affiliates to after log on (specified group(s)/ N/A)
[R-6.4.2-006]	Authorisation of a user to request a list of which groups a user has affiliated to
[R-6.4.6.1-002] [R-6.4.6.1-003]	Authorisation to change affiliated groups of other specified user(s)
[R-6.4.6.2-001] [R-6.4.6.2-002]	Authorisation to recommend to specified user(s) to affiliate to specific group(s)
[R-6.6.1-004]	Authorisation to perform regrouping
[R-6.7.2-001]	Presence status is available/not available to other users
[R-6.7.1-002] [R-6.7.2-002]	Authorisation to obtain presence of user (list of users)
[R-6.7.2-003]	User is able/ unable to participate in private calls
[R-6.7.1-004] [R-6.7.2-003] [R-6.7.2-004]	Authorisation to query whether MCPTT User is available for private calls
[R-6.7.1-010]	Authorisation to override transmission in a private call
[R-6.7.1-013]	Authorisation to restrict provision of private call set-up failure cause to the caller
[R-6.8.7.4.2-001] [R-6.8.7.4.2-002]	Authorisation of a user to cancel an emergency alert on any MCPTT UE of any user
[R-6.13.4-001]	Authorisation for a user to enable/disable a user
[R-6.13.4-003] [R-6.13.4-005] [R-6.13.4-006] [R-6.13.4-007]	Authorisation for a user to (permanently /temporarily) enable/disable a UE
[R-6.2.3.4-001]	Authorisation to revoke permission to transmit
[R-7.14-002] [R-7.14-003]	Authorization for manual switch to off-network while in on-network

Table B.3-3: User configuration data / MCPTT user profile data (off network)

Reference	Parameter description
[R-7.2-003]	List of off-network MCPTT groups for use by an MCPTT user
[R-7.3.3-008]	Allowed listening of both overriding and overridden
[R-7.3.3-006]	Allowed transmission in case of override (overriding and/or overridden)
[R-7.8.1-001]	Authorization for participant to change an off-network group call in-progress to off-network emergency group call
[R-7.8.3.1-003]	Authorization for participant to change an off-network group call in-progress to off-network imminent peril group call
[R-7.12-002] [R-7.12-003]	Authorization for off-network services

B.4 Group configuration data

Data in table B.4-1, B.4-2 and B.4-3 has to be known by the MCPTT UE and MCPTT server associated to MCPTT ID. CSC-2 reference point is used for configuration between group management server and MCPTT UE when the UE is on-network. CSC-3 reference point is used for configuration between group management server and MCPTT server.

Data in table B.4-1 and B.4-3 can be configured offline using the CSC-12 interface. Tables B.4-1 and B.4-3 are the UE configuration required to support the use of off-network MCPTT service.

Table B.4-1: Group configuration data (on and off network)

Reference	Parameter description
[R-5.19-004] [R-6.4.3-001] [R-6.4.3-002] [R-6.9-004] [R-5.1.3-002]	MCPTT group ID
[R-5.19-004] [R-6.4.3-001] [R-6.4.3-002] [R-6.9-004]	Group Alias (Contact URIs)
[R-5.1.3-001] [R-5.1.5-001] [R-6.4.5-005] [R-6.4.5-006]	List of group members (group membership information): - MCPTT ID (group membership information) - User priority for the group (group membership information) - Participant type for the group (group membership information)
[R-5.18.2-001] [R-5.18.2-002]	Group"s owner (Mission Critical Organisation)
[R-5.1.7-002] [R-6.2.2-001] [R-6.6.2.2-006] [R-6.8.6.2-003]	Priority of the group
[R-5.7.2.1.2-002]	Timeout value for the cancellation of an in progress emergency for a group call
[R-5.7.2.2.2-004]	Timeout value for the cancellation of an in progress imminent-peril group call
[R-6.4.9-006] [R-5.14-001]	Preferred voice codecs for MCPTT group
[R-5.2.2-001]	Level within group hierarchy (only applicable for group-broadcast group)
[R-5.2.3-001]	Level within user hierarchy (only applicable for user-broadcast group)
[R-5.7.2.1.1-013] [R-5.7.2.4.1-008]	Indication whether emergency group call is permitted on the MCPTT group
[R-5.7.2.2.1-009]	Indication whether imminent peril group call is permitted on the MCPTT group
[R-5.7.2.4.1-012]	Indication whether emergency alert is possible on the MCPTT group

Table B.4-2: Group configuration data (on network)

Reference	Parameter description
[R-6.2.4-003] [R-6.4.9-002]	Group call hang timer
[R-5.1.6-001] [R-6.4.9-003]	Maximum duration of group calls
Subclause 10.6.2	Group call model used for group (chat/ pre-arranged)
Subclause 10.6.2.4.1	Temporary group indication
[R-6.1-001]	Maximum number of group members (N11)
[R-6.2.1-004] [R-6.2.1-007]	Minimum number of affiliated group members acknowledging before start of audio transmission
[R-6.2.1-005] [R-6.2.1-007]	List of group members which have to acknowledge before start of audio transmission NOTE: Listed group members will be automatically affiliated for the duration of this group call if not already affiliated
[R-6.2.1-006] [R-6.2.1-007]	Geographical area where acknowledgement of all affiliated group members is required before start of audio transmission
[R-6.2.1-008] [R-6.2.1-009]	Timeout for acknowledgement of required group members
[R-6.2.1-008] [R-6.2.1-009] [R-6.2.1-012]	Action upon failure to receive acknowledgement from required group members before call timeout (proceed or abandon)
[R-6.4.9-005]	List of group members with receive-only participant type
[R-6.6.2.2-003] [R-6.6.2.2-004]	The security level of the group
[R-6.1-003]	Enabled/disabled group (basic status)
[R-6.4.5-005]	Authorisation to request list of members of an MCPTT group
[R-6.4.5-001] [R-6.4.5-003]	Authorisation of a user to request a list of affiliated members of a group

Table B.4-3: Group configuration data (off network)

Reference	Parameter description
Subclause 8.1.3.2	Prose layer-2 group ID
Subclause 8.1.3.2	ProSe group IP multicast address
Subclause 10.1.3.3	Associated relay service code
[R-7.4-002]	Group call hang timer
[R-7.4-003]	Max duration of group calls
Subclause 10.1.5.4	ProSe user info id (group membership information)

B.5 Service configuration data

Data in table B.5-1 has to be known by the MCPTT server. CSC-3 reference point is used for configuring data from group management server. CSC-5 reference point is used for configuring from configuration management server.

Editor's note: A reference point is required to be defined for offline service configuration for tables B5.1 and B5.3.

Table B.5-1: Service configuration data (on and off network)

Reference	Parameter description
[R-5.7.2.3.2-002]	Timeout value for the cancellation of an in progress emergency for a private call
[R-5.7.2.1.2-002]	Time limit for an In-progress emergency related to an MCPTT group
[R-5.6.5-004]	Max private call (with floor control) duration
[R-5.2.2-001]	Levels of group hierarchy for group-broadcast groups (B1)
[R-5.2.3-001]	Levels of user hierarchy for user-broadcast groups (B2)
[R-5.8-002]	Minimum length (N3) of an alphanumeric identifier (i.e., alias) assigned by an MCPTT administrator.

Table B.5-2: Service configuration data (on network)

Reference	Parameter description
[R-6.2.4-003]	Hang timer for private calls
[R-6.7.2-008]	Max duration of private call (without floor control)
[R-6.2.3.3.1-001] [R-7.3.3-002]	Hierarchy of participant rights to override
[R-6.2.3.5-002]	Transmit time limit from a single request to transmit in a group or private call transmission
[R-6.2.3.5-003] [R-6.2.3.5-004]	Configuration of warning time before time limit of transmission is reached (on-network)
[R-6.2.4-005]	Configuration of warning time before call hang time (on-network)
[R-6.2.3.2-006]	Depth of floor control queue
[R-6.2.3.2-012]	Max time for a user's floor control request to be queued

Table B.5-3: Service configuration data (off network)

Reference	Parameter description
[R-7.4-002] [R-7.4-003]	Hang timer for private calls in off-network
[R-7.3.3-001] [R-7.3.3-002] [R-7.3.3-003]	Priority hierarchy for floor control override in off-network
[R-7.3.5-001] [R-7.3.5-002] [R-7.3.5-003]	Transmit time limit from a single request to transmit in a group or private call.
[R-7.3.5-001] [R-7.3.5-004]	Configuration of warning time before time limit of transmission is reached (off-network)
[R-7.4-004]	Configuration of warning time before hang time is reached (off-network)
[R-7.7-001] [R-7.7-002] [R-7.7-003]	Call priority configuration NOTE: This needs to be mapped to ProSe per packet priorities
[R-7.15-001]	Configuration of metadata to log

B.6 Initial configuration data

The initial configuration data are essential by the UE to successfully connect to and use the MCPTT service. The initial configuration data may include information like default user profile and identities of the application servers (e.g., group management server, configuration management server, identity management server).

Annex C (informative): Local UE settings for MCPTT

C.1 Local UE settings for MCPTT

Table C.1-1 details local UE settings for MCPTT that represent important functionalities that may be required by MCPTT UEs, however these functionalities do not require central configuration like the parameters in annex B, so these are detailed in this annex for information to UE vendors interested in producing MCPTT UEs. The various columns in the tables have the following meanings:

- Reference: Is the reference of the corresponding requirement in 3GPP TS 22.179 [2].
- Definition: A short definition of the local UE setting.

Table C.1-1: Local UE settings for MCPTT

Reference	Definition
5.1.1-003	Call reception signalling method
5.1.1-004	Disabling of call reception signalling
5.8-003	Configuration of display of User ID (on/off)
5.8-003	Configuration of display of aliases associated with the User ID (on/off)
5.8-003	Configuration of display of Selected MCPTT Group (on/off)
5.8-003	Configuration of display of Mission Critical Organization name (on/off)
6.8.7.4.1-003	Configuration of the notification of an emergency alert

Annex D (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2015-05						Initial version.	-	0.0.0
2015-06	SA6#4					Implementation of the following p-CRs approved by SA6: S6-150459 (scope); S6-150460 (skeleton and transfer of material from 3GPP TR 23.779).	0.0.0	0.1.0
2015-06	e-mail review					Incorporation of visio diagrams for figures 10.6.3-1, 10.6.4-1, 10.7.1-1, 10.7.3-1, 10.7.5-1, 10.7.6-1, 10.8-1 and 10.8-2.	0.1.0	0.1.1
2015-07	SA6#5					Implementation of the following p-CRs approved by SA6: S6-150499; S6-150531; S6-150538; S6-150578; S6-150579; S6-150587; S6-150599; S6-150603; S6-150608;S6-150609; S6-150611; S6-150612; S6-150642; S6-150644; S6-150645; S6-150646; S6-150651; S6-150652; S6-150653; S6-150654; S6-150655; S6-150661; S6-150669; S6-150670; S6-150671; S6-150672; S6-150677; S6-150679; S6-150681; S6-150682; S6-150683; S6-150684; S6-150685; S6-150686; S6-150689; S6-150690; S6-150697; S6-150698; S6-150699; S6-150701; S6-150702; S6-150703; S6-150704; S6-150716; S6-150718; S6-150719; S6-150728; S6-150729; S6-150730; S6-150731; S6-150732; S6-150733; S6-150734; S6-150735; S6-150737; S6-150739; S6-150740; S6-150741; S6-150742; S6-150743; S6-150744; S6-150745; S6-150747; S6-150749; S6-150750.	0.1.1	0.2.0
2015-08	SA6#6					Implementation of the following p-CRs approved by SA6: S6-150770; S6-150773; S6-150776; S6-150783; S6-150814; S6-150816; S6-150818; S6-150823; S6-150832; S6-150834; S6-150859; S6-150860; S6-150867; S6-150881; S6-150882; S6-150883; S6-150888; S6-150898; S6-150899; S6-150901; S6-150903; S6-150904; S6-150905; S6-150908; S6-150909; S6-150917; S6-150926; S6-150927; S6-150931; S6-150932; S6-150934; S6-150936; S6-150937; S6-150938; S6-150939; S6-150940; S6-150941; S6-150944; S6-150945; S6-150946; S6-150950; S6-150951; S6-150953; S6-150954; S6-150955; S6-150958; S6-150959; S6-150960; S6-150962; S6-150964; S6-150966; S6-150967; S6-150983; S6-150984; S6-150986; S6-150987; S6-150988; S6-150989; S6-150990.	0.2.0	0.3.0
2015-08	e-mail review					Implementation of S6-150973 which was approved at SA6#6.	0.3.0	0.4.0
2015-09	SA#69	SP-150485				Submitted to SA#69 for information	0.4.0	1.0.0
2015-10	SA6#7					Implementation of the following p-CRs approved by SA6: S6-150995; S6-151004; S6-151021; S6-151024; S6-151031; S6-151092; S6-151115; S6-151176; S6-151184; S6-151185; S6-151190; S6-151192; S6-151197; S6-151199; S6-151200; S6-151204; S6-151205; S6-151206; S6-151210; S6-151213; S6-151216; S6-151217; S6-151218; S6-151219; S6-151220; S6-151221; S6-151222; S6-151223; S6-151224; S6-151229; S6-151232; S6-151234; S6-151236; S6-151237; S6-151238; S6-151242;	1.0.0	1.1.0

						S6-151243; S6-151244; S6-151249; S6-151251; S6-151253; S6-151256; S6-151257; S6-151261; S6-151262; S6-151263; S6-151265; S6-151266; S6-151267; S6-151268; S6-151271; S6-151272; S6-151275; S6-151276; S6-151277; S6-151281; S6-151285; S6-151286; S6-151287; S6-151288; S6-151289; S6-151290; S6-151294; S6-151295; S6-151297; S6-151298; S6-151299; S6-151300; S6-151301; S6-151302; S6-151303; S6-151304; S6-151305; S6-151306; S6-151308; S6-151309; S6-151310; S6-151311; S6-151312; S6-151314; S6-151315; S6-151316; S6-151317; S6-151319; S6-151320; S6-151322; S6-151323.		
2015-10	e-mail review					Correct implementation for S6-151319	1.1.0	1.1.1
2015-12	SA6#8					Implementation of the following p-CRs approved by SA6: S6-151326; S6-151338; S6-151351; S6-151352; S6-151353; S6-151357; S6-151364; S6-151448; S6-151461; S6-151469; S6-151470; S6-151473; S6-151482; S6-151484; S6-151486; S6-151489; S6-151490; S6-151491; S6-151497; S6-151498; S6-151500; S6-151501; S6-151503; S6-151504; S6-151509; S6-151513; S6-151515; S6-151517; S6-151520; S6-151523; S6-151524; S6-151526; S6-151528; S6-151529; S6-151530; S6-151531; S6-151533; S6-151534; S6-151535; S6-151536; S6-151537; S6-151538; S6-151539; S6-151542; S6-151543; S6-151545; S6-151546; S6-151548; S6-151549; S6-151550; S6-151551; S6-151552; S6-151554; S6-151555; S6-151557; S6-151558; S6-151559; S6-151560; S6-151561; S6-151562; S6-151563; S6-151564; S6-151565; S6-151566; S6-151567.	1.1.1	1.2.0
2015-12	SA#70	SP-150733				Submitted for Approval at SA#70	1.2.0	2.0.0
2015-12	SA#70	SP-150733				MCC Editorial update for publication after TSG SA approval (SA#70)	2.0.0	13.0.0

History

Document history		
V13.0.0	January 2016	Publication