ETSI TS 123 280 V14.2.0 (2017-07)

LTE;
Common functional architecture to support mission critical services;
Stage 2
(3GPP TS 23.280 version 14.2.0 Release 14)

Reference
RTS/TSGS-0623280ve20

Keywords
LTE

ETSI

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

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

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

Intellectual Property Rights

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 common functional architecture, procedures and information flows needed to support mission critical services including the common services core architecture.

The corresponding service requirements are defined in 3GPP TS 22.179 [2], 3GPP TS 22.280 [3], 3GPP TS 22.281 [4] and 3GPP TS 22.282 [5].

The present document is applicable primarily to mission critical services using E-UTRAN access based on the EPC architecture defined in 3GPP TS 23.401 [17]. Certain MC service 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 common functional architecture to support mission critical services can be used for public safety applications and also for general commercial applications e.g. utility companies and railways.

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 22.280: "Mission Critical Services Common Requirements (MCCoRe); Stage 1".

[4] 3GPP TS 22.281: "Mission Critical Video services over LTE".

[5] 3GPP TS 22.282: "Mission Critical Data services over LTE".

[6] 3GPP TS 23.002: "Network Architecture".

[7] 3GPP TS 23.179: "Functional architecture and information flows to support mission critical communication services; Stage 2"

[8] 3GPP TS 23.203: "Policy and charging control architecture".

[9] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[10] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 2".

[11] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[12] 3GPP TS 23.281: "Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2".

[13] 3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2".

[14] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[15] 3GPP TS 23.335: "User Data Convergence (UDC); Technical realization and information flows".

[16] 3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".

[17] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[18] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE); Stage 2".

[19] 3GPP TS 29.283: "Diameter Data Management Applications".

[20] 3GPP TS 33.179: "Security of Mission Critical Push-To-Talk (MCPTT)".

[21] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

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

[23] GSMA PRD IR.92 v10.0: "IMS Profile for Voice and SMS".

[24] GSMA PRD IR.88 v15.0: "LTE and EPC Roaming Guidelines".

[25] 3GPP TS 33.180: "Security of the mission critical service".

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].

Active MC service user profile: The MC service user profile that is currently used by an MC service client of an MC service user while receiving MC service.

Location: The current physical location of the MC service UE.

MC service: A generic name for any one of the three mission critical services: either MCPTT, or MCVideo, or MCData.

MC service affiliated group member: An MC service user who has indicated an interest in a particular MC service group and has been accepted to participate in MC service group communication for that MC service group.

MC service client: A generic name for the client application function of a specific MC service. MC service client could be replaced by MCPTT client, or MCVideo client, or MCData client depending on the context.

MC service group: A defined set of MC service users with associated communication dispositions (e.g. media restrictions, default priority and commencement directions) configured for the use with one or more MC services.

MC service group affiliation: A mechanism by which an MC service user's MC service(s) communication interest in one or more MC service groups is determined.

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

MC service group de-affiliation: A mechanism by which an MC service user's MC service(s) communication interest in one or more MC service groups is removed.

MC service group home system: The mission critical system where the MC service group is defined.

MC service group host MC service server: The MC service server within a mission critical system which provides centralised support for a particular MC service of an MC service group defined in a MC service group home system.

MC service group member: An MC service user, whose MC service ID is listed in a particular MC service group.

MC service ID: A generic name for the user ID of a mission critical user within a specific MC service. MC service ID could be replaced by MCPTT ID, or MCVideo ID, or MCData ID depending on the context.

MC service server: A generic name for the server application function of a specific MC service. MC service server could be replaced by MCPTT server, MCVideo server, or MCData server depending on the context.

MC service user: An authorized user, who can use an MC service UE to participate in one or more MC services.

MC service user profile: The set of information associated to an MC service user that allows that user to employ one or more MC services in a given role and from a given MC service UE.

MC service UE: A UE that can be used to participate in one or more MC services.

MC user: A user, identified by an MC ID, who, after authorization, obtains mission critical service(s).

Mission critical system: The collection of applications, services, and enabling capabilities required to provide a single mission critical service or multiple mission critical services to one or more mission critical organizations.

Pre-selected MC service user profile: The MC service user profile that is to be selected as the active MC service user profile through configuration, and applicable for an authenticated MC service user upon MC service authorization.

Selected MC service user profile: The MC service user profile that is to be selected as the active MC service user profile for an MC service upon request by an MC service user.

For the purposes of the present document, the following terms given in 3GPP TS 22.280 [3] apply

Mission Critical
Mission Critical Applications
Mission Critical Organization
Mission Critical Service

3.2 Symbols

For the purposes of the present document, the symbols given in 3GPP TS 22.280 [3] apply

Nc6

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
BM-SC	Broadcast Multicast Service Centre
CSC	Common Services Core
CSCF	Call Server Control Function
DPF	Direct Provisioning Function
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
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
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
I-CSCF	Interrogating CSCF
IARI	IMS Application Reference Identifier
ICE	Interactive Connectivity Establishment

ICSI	IMS Communication Service Identifier
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 AS	MCPTT Application Server
MCPTT ID	MCPTT user identity
NAT	Network Address Translation
P-CSCF	Proxy CSCF
PLMN	Public Land Mobile Network
ProSe	Proximity-based Services
PSI	Public Service Identity
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
S-CSCF	Serving CSCF
SIP	Session Initiated Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TMGI	Temporary Mobile Group Identity
UDC	User Data Convergence
UDR	User Data Repository
USB	Universal Serial Bus
URI	Uniform Resource Identifier
WLAN	Wireless Local Area Network

For the purposes of the present document, the abbreviations given in 3GPP TS 22.280 [3] apply

MCData
MCPTT
MCVideo

4 Introduction

A common functional architecture to support MC services (i.e., MCPTT defined in 3GPP TS 23.379 [16], MCVideo defined in 3GPP TS 23.281 [12], MCData defined in 3GPP TS 23.282 [13]) including common application plane and signalling plane entities is specified in this document.

Each MC service supports several types of communications amongst the users (e.g. group call, private call). There are several common functions and entities (e.g. group, configuration, identity) which are used by the MC services.

The common functional architecture to support MC services utilises aspects of the IMS architecture defined in 3GPP TS 23.228 [9], the Proximity-based Services (ProSe) architecture defined in 3GPP TS 23.303 [14], the Group Communication System Enablers for LTE (GCSE_LTE) architecture defined in 3GPP TS 23.468 [18] and the PS-PS access transfer procedures defined in 3GPP TS 23.237 [10].

The MC service UE primarily obtains access to a MC service via E-UTRAN, using the EPS architecture defined in 3GPP TS 23.401 [17]. Certain MC service functions such as dispatch and administrative functions can be supported using either MC service UEs in E-UTRAN or using MC service UEs via non-3GPP access networks. External applications usage of MC services can be enabled via E-UTRAN or non-3GPP access networks.

NOTE: Dispatch consoles and devices used by MC service administrators are considered MC service UEs in the common functional architecture to support MC services.

5 Assumptions and architectural requirements

5.1 Assumptions

5.1.1 Service continuity

Service continuity shall be supported between on-network MC services and UE-to-network relay MC services. The following 3GPP TS 23.237 [9] procedures are needed:

- Originating sessions that use only PS media flow(s) as defined in subclause 6.2.1.3.
- Terminations sessions that use only PS media flow(s) as defined in subclause 6.2.2.3.
- Remote Leg Update as defined in subclause 6.3.1.5.
- PS-PS Access Transfer with full media transfer as defined in subclause 6.2.2.1.

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

5.1.2 Trust domain

For an MC system, the trust domain consists of one or more MC service functions that are administered by the same or different service providers (e.g. MC service provider, PLMN operator) that have an agreement to share sensitive information.

For the MC system architecture, the following rules are implied for functions in different trust domains:

- A public user identity shall not identify an MC service user in a different trust domain (see subclause 8.3.1);
- A public service identity shall not identify an MC service group ID in a different trust domain (see subclause 8.3.2);
- A SIP database shall not pass responses to a registrar or registrar finder in a different trust domain (see subclause 7.4.3.2.1); and
- An HTTP proxy shall not pass requests or responses to another HTTP proxy, an HTTP server or an HTTP client in a different trust domain (see subclause 7.4.3.3.2).

5.2 Architectural requirements

5.2.1 General architectural requirements

General MC service architectural requirements include:

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

   Hence a functional decomposition of MC service architecture into distinct logical functions is required.

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

c) To enable parts of the MC service architecture to be shared for other applications, the architecture should enable the group management functions (e.g. admission control; linking of groups;) to be implemented on a separate node from the main application functions of the MC service (e.g. "call" setup/termination; allocation of TMGI to UE; floor control;).

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

5.2.2 Roaming requirements

The MC applications can provide MC services to users in various PLMNs. Roaming is supported using EPC-level roaming or IMS-level roaming.

5.2.3 UE-to-network relay MC 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 MC service should be able to provide a means for an MC service administrator to configure a ProSe UE-to-network relay with a list of allowed MC service groups. For each allowed MC service group, a unique associated relay service code should be allocated and it may be provided to the relay UE from MC service server or DPF.

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

5.2.4 MC service user profile requirements

The MC service user profile shall:

- be provisioned subject to the user authentication by the identity management server;
- be available at configuration management server;
- be available at MC service servers with the corresponding user profile information;
- be associated with an MC service user; and
- contain an index to uniquely distinguish the MC service user profile from other MC service user profiles associated to the same MC service user.

For the set of MC service user profiles associated to a single MC service user, one of the MC service user profiles shall be indicated as the pre-selected MC service user profile to the MC service client and the MC service server.

The MC service user shall be able to:

- change the pre-selected MC service user profile; and
- change the selected MC service user profile.

The MC service user profile may be modified at the configuration management server.

5.2.5 MC service group affiliation and MC service group de-affiliation

The MC system shall support affiliation and de-affiliation to an MC service group for one or more MC services. For affiliation and de-affiliation, the MC service client shall indicate interest in one or more MC services for the MC service group. For a single MC service group configured for multiple MC services, the affiliation and de-affiliation shall be performed as per the MC service selected by the MC service user. For individual MC service group affiliation and MCservice group de-affiliation, the requirements are specified in the corresponding MC service TS.

Editor’s note: The requirement for a combined affiliation to multiple MC services for a single MC service group is FFS.

MC service group affiliation can be achieved through the following two methods:

a) Explicit affiliation: An MC service client indicates interest in one or many MC service groups to the MC service server. This interest may be initiated either by an MC service user using the MC service UE, or by an automatic procedure within the MC service client that indicates that the MC service user is interested in the MC service

group at that MC service client. An authorized MC service user may remotely modify another MC service user's affiliation to an MC service group.

b) Implicit affiliation: An MC service user's affiliations to MC service groups are determined through configurations and policies within the MC service and performed by the associated MC service server.

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

The MC service server may refuse a request for affiliation from an MC service user to an MC service group, in which case the MC service user will be unable to take part in the requested MC service associated with that MC service group, and the MC service client should make the MC service user aware that the MC service user is not affiliated to the MC service group for the requested MC service. The MC service server may also de-affiliate an MC service client from an MC service group following a relevant trigger condition.

MC service group de-affiliation indicates that the MC service user is no longer interested in that MC service group, either at the MC service client, or across all MC service clients depending on MC service group configuration, and therefore is unable to perform any actions that are associated with an affiliated member (e.g. receive media, notifications). MC service group de-affiliation can occur due to either an MC service client's explicit request, or implicitly i.e. changed by the MC service server as the result of another action e.g. the MC service user logging off.

5.2.6 GCS AS requirements for the MC services

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. The MC service on-network architecture, is based in part on 3GPP TS 23.468 [18] with the MC service server assuming the function of the GCS AS and can be represented (in a simplified diagram) as shown in figure 5.2.6-1:

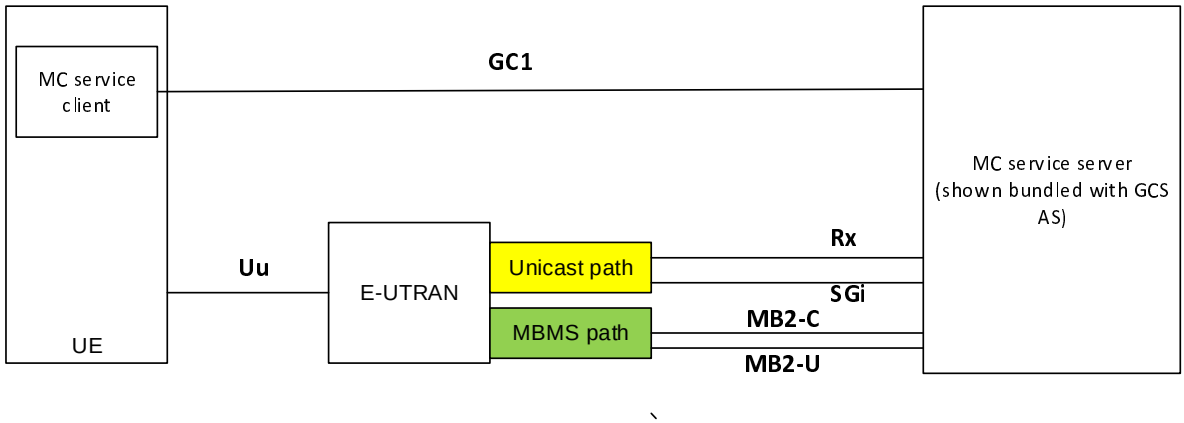

Figure 5.2.6-1: MC service on-network architecture showing MBMS

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

MC service media content is transmitted via LTE bearers, which are communication pipes with one end in the MC service server and the other end in the MC service 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 [11]). The MC service 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 [18]). The MC service server may determine the MBMS broadcast area based on the cell identities of the affiliated group members received over GC1. The MC service server may determine for a user the switching from MBMS bearer to unicast bearer based on the information reported over GC1.

5.2.7 Bearer management

5.2.7.0 General

The MC service UE shall use the following APNs:

- an MC services APN for the SIP-1 reference point;
- an MC common core services APN for the HTTP-1 reference point; and
- an MC identity management service APN for the CSC-1 reference point.

The value of each of these APNs:

- may be the same or may differ;
- may be the same as other non-MC services that have compatible QoS and PDN (see NOTE); and
- shall be made available to the UE either via UE (pre)configuration or via initial UE configuration (see subclause 10.1.1) on a per HPLMN and optionally also a per VPLMN basis.

NOTE: The APN value of "IMS" is a well-known APN, whose PDN connection characteristics are defined in GSMA PRD IR.92 [23] and GSMA PRD IR.88 [24], and which is used in some deployments for operator IMS-based services e.g. Voice over LTE. This well-known APN can be used for the MC service APN if the SIP core belongs to the PLMN operator and both the PLMN operator and MC service provider have agreed which QoS aspects to utilise i.e. either the QoS aspects defined in subclause 5.2.7.2 or the QoS aspects defined in GSMA PRD IR.92 [23] and GSMA PRD IR.88 [24].

The MC service UE may utilise PDN access credentials as specified in 3GPP TS 23.401 [17] (e.g. PAP, CHAP) to access the PDNs identified by the MC service APN, the MC common core services APN and the MC identity management service APN. If PDN access credentials are required, then they shall be made available to the MC service UE via initial MC service UE configuration (see subclause 10.1.1) on a per APN basis.

The PDN connection to the APNs defined within the present subclause can be of type "IPv4", "IPv6" or "IPv4v6" (see 3GPP TS 23.401 [17]). If a PDN connection to an APN defined within the present subclause is of type "IPv4v6" then the MC service client shall use configuration data to determine whether to use IPv4 or IPv6.

5.2.7.1 MBMS bearer management

When operating in systems that support MBMS functionality, the MC service can provide downlink MBMS delivery of MC service media.

When operating in systems that support MBMS functionality, the MC service can provide downlink MBMS delivery of application level control messages targeted towards multiple MC clients at the same time (e.g. floor idle and floor taken for MCPTT services).

MC service UEs can receive the traffic delivered via MBMS, regardless of whether or not they have any unicast radio bearers available.

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

The MC service shall enable an MC service UE in an ongoing MC service group session that has just entered an area of media delivery via MBMS bearers to immediately start receiving the media for that MC service group session via MBMS.

The MC service server shall not map MC service group sessions to MBMS bearers that cannot provide the QoS required by the group.

An MC service UE that uses MBSFN transmission should be able to support eight MBSFN areas simultaneously on the same RF carrier.

5.2.7.2 EPS bearer considerations

5.2.7.2.1 Considerations for the EPS bearer to the MC services PDN

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

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

5.2.7.2.2 Considerations for the EPS bearer to the MC common core services PDN and MC identity management service PDN

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

5.2.8 External applications access to services in a MC system

The MC system shall allow external applications to gain secure access to MC services by supporting authentication and authorization of external applications.

Editor's Note: External applications reside outside a MC system and can access a MC system using IP connectivity.

Editor's Note: How to enable the external application access to services in an MC system is FFS.

Editor's Note: The definition for services and capabilities discovery is FFS.

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 MC service user.

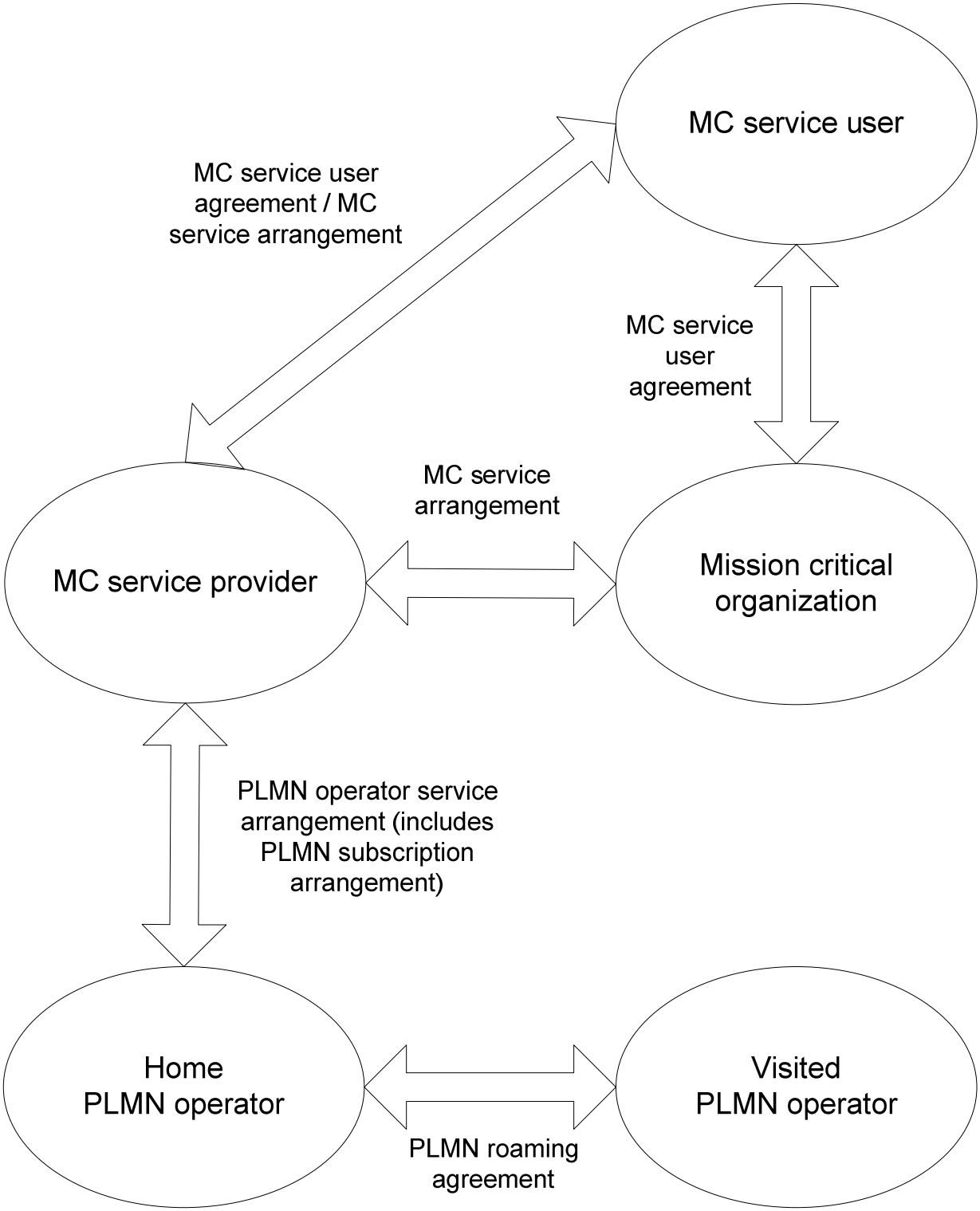

Figure 6-1: Business relationships for MC services

The MC service user belongs to a single mission critical organization based on a MC service user agreement between the MC service user and the mission critical organization. The MC service user can have MC service user agreement and MC service arrangement directly with a single MC service provider.

The mission critical organization and the MC service provider can be part of the same organization, in which case the business relationship between the two is internal to a single organization. The mission critical organization can have MC service arrangements with several MC service providers. In this case, a MC service user of a mission critical organization is always served by only one MC service provider. The MC service provider can have MC service arrangements with several mission critical organizations. The MC service provider can have MC service user agreements and MC service arrangements with several MC service users.

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

The home PLMN operator can have PLMN operator service arrangements with multiple MC service providers and the MC service provider can have PLMN operator service arrangements with multiple home PLMN operators. As part of the PLMN operator service arrangement between the MC service provider and the home PLMN operator, PLMN subscription arrangements can be provided which allows the MC service UEs to register with home PLMN operator network.

The home PLMN operator can have PLMN roaming agreements with multiple visited PLMN operators and the visited PLMN operator can have PLMN roaming agreements with multiple home PLMN operators.

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

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

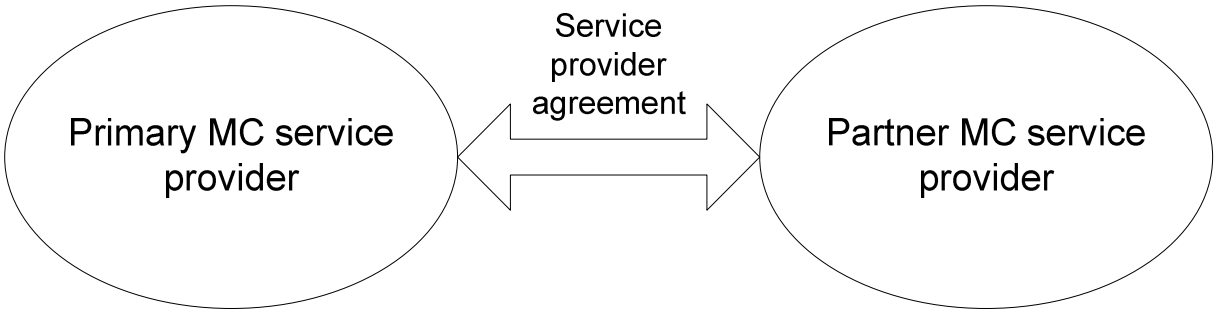

Figure 6-2: Additional business relationships for mutual aid

The primary and partner MC 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 MC service provider and one providing mutual aid within the same group:

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

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

b) user A uses a PLMN subscription arrangement with PLMN operator R provided by MC service provider X; and

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

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

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

b) user B uses a PLMN subscription arrangement with PLMN operator S provided by MC service provider Y;

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

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

e) PLMN operator S has a PLMN 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 MC service provider X has a service arrangement with. It does however need to support one or more MC services capabilities, and provides service in the same geographic area as used by MC service provider X.

7 Functional model

7.1 General

The functional model for the MC services architecture 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, video control, data control) required by the user together with the necessary functions to support MC service. It uses the services of the signalling control plane to support those requirements. For example, within the MCPTT service, the application plane also provides for the conferencing 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 MC service, such as an MCPTT call or other type of MC services. The signalling control plane also offers access to and control of services across MC services. The signalling control plane uses the services of the bearer plane.

Bearers supporting these planes are defined for LTE within 3GPP TS 23.401 [17]. The resource control that is needed to support these planes is defined within 3GPP TS 23.203 [8]. The application plane also relies on the use of multicast bearers established via procedures defined in 3GPP TS 23. 468 [18] and 3GPP TS 23.246 [11].

7.3 Functional model description

7.3.1 On-network functional model

Each MC service can be represented by an application plane functional model. The functional model across MC services may be similar but is described by the individual functional entities and reference points that belong to that MC service. Within the application plane for an MC service there is a common set of functions and reference points. The common set is shared across services. This common set of functions and reference points is known as the common services core.

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

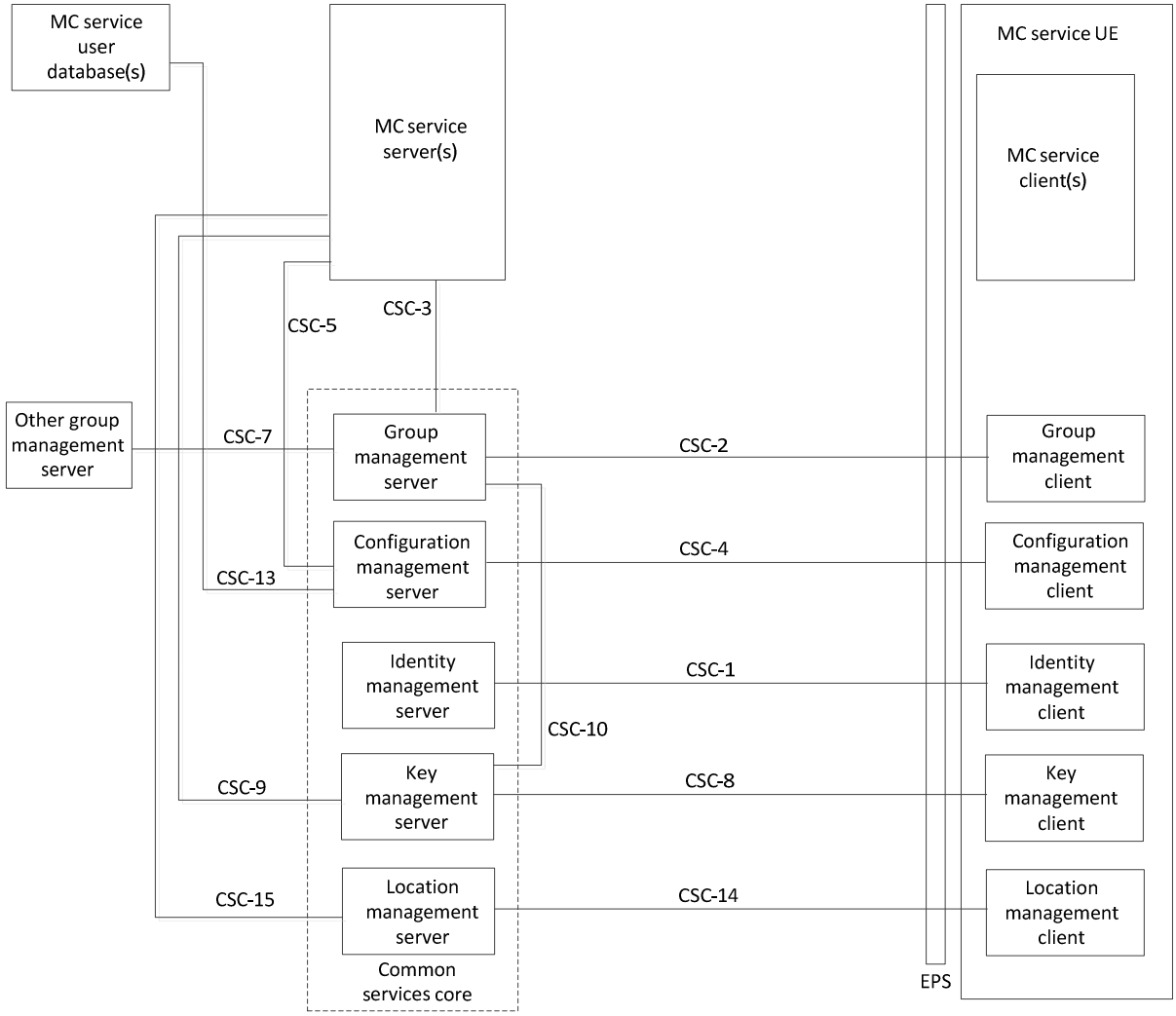

Figure 7.3.1-1: Functional model for application plane for an MC system

The common services core functions and reference points shown in figure 7.3.1-1 are shared across each MC service. The description of the functions and reference points specific to an MC service is contained in the corresponding MC service TS.

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

- A specific MC service server is an instantiation of a GCS AS in accordance with 3GPP TS 23.468 [18].

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

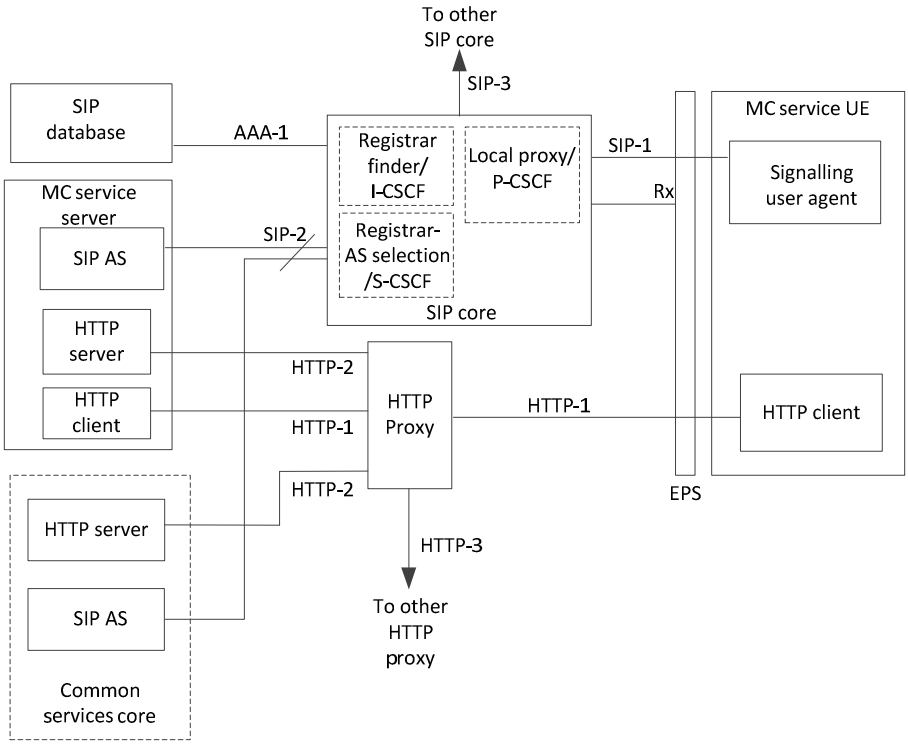

Figure 7.3.1-2: Functional model for signalling control plane

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

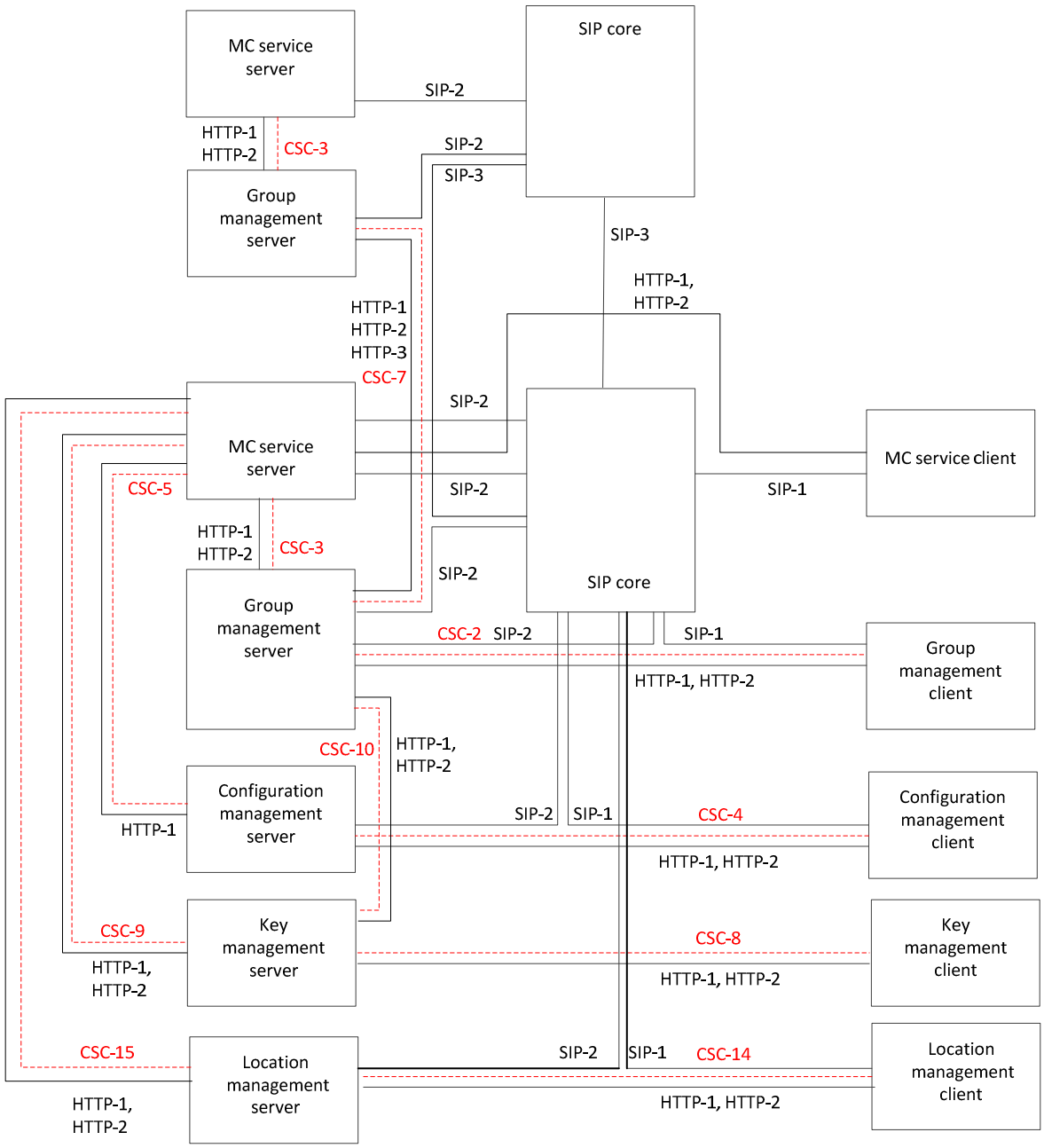

Figure 7.3.1-3: Relationships between reference points of MC service application plane and signalling control planes

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.

NOTE 3: CSC-5, CSC-9, and CSC-15 make use of SIP-1 and SIP-2 reference points. For simplicity, this mapping relationship 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.

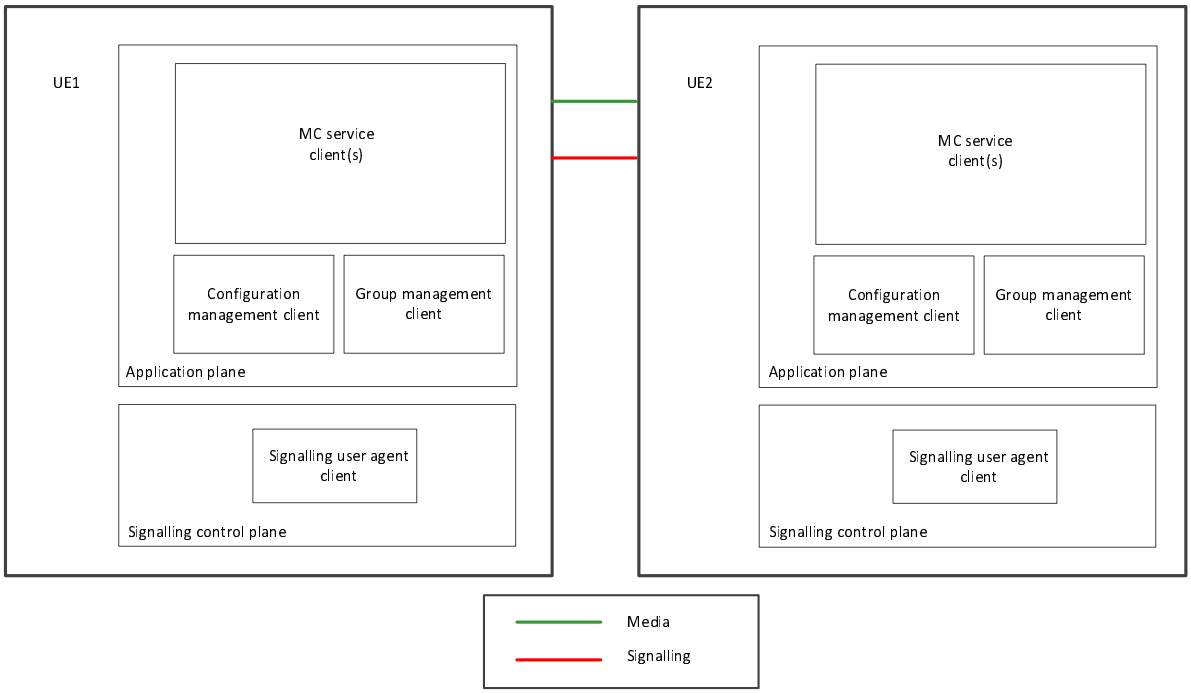

Figure 7.3.2-1: Functional model for MC service off-network operation

For a specific MC service, the description of off-network operation is contained in the corresponding MC service TS.

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 of an MC system provide application control and media specific functions to support one or more MC services.

For each MC service, the functional entities description is contained in the corresponding MC service TS.

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 one or more MC service applications with non-group management MC service related information and configure data on the configuration management client. The configuration management server manages MC service configuration supported within the MC 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 groups. A MC system maintains groups corresponding to one or more mission critical organizations. The group management client 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 MC 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 processing.

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 MC system.

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 [20].

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 MC service server(s) 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 [20].

7.4.2.2.9 Location management client

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

7.4.2.2.10 Location management server

The location management server is a functional entity that receives and stores user location information, and provides user location information to the MC service server. The location management server may also acquire location information provided by PLMN operator.

Editor's Note: How to resolve the identity used for the location management server to acquire the location of MC service user from the PLMN operator is FFS.

7.4.2.3 MC service

7.4.2.3.1 MC service client

The MC service client functional entity acts as the user agent for all MC service transactions. For a specific MC service, the detailed description of functions of the MC service client is contained in the corresponding MC service TS.

7.4.2.3.2 MC service server

The MC service server functional entity provides centralised support for MC services.

The MC service server functional entity represents a specific instantiation of the GCS AS described in 3GPP TS 23.468 [18] to control multicast and unicast operations for group communications. For a specific MC service, the detailed description of the GCS AS role assumed by the MC service server is contained in the corresponding MC service TS.

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

7.4.2.3.3 MC service user database

This functional entity contains information of the MC service user profile associated with an MC service ID that is held by the MC service provider at the application plane. The MC service user profile is determined by the mission critical organization, the MC service provider, and potentially the MC service user.

Each MC service shall have a corresponding MC service user database i.e. MCPTT user database as defined in 3GPP TS 23.379 [16], MCVideo user database as defined in 3GPP TS 23.281 [12] and MCData user database as defined in 3GPP TS 23.282 [13]. These MC service user databases can be co-located.

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 MC service:

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

NOTE: In the IM CN subsystem, this is provided by the Application Server as defined in 3GPP TS 23.002 [6].

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 [9], 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 [9], 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 [6].

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 MC service provider. In this case, the source of the data may be the MC service provider's SIP database.

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 [9].

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 MC 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 MC service provider domain: registrar finder in the MC service provider's domain uses the information from the MC service provider's SIP database to identify the serving registrar in the MC 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 MC service provider domain: registrar finder uses information from the MC service provider's SIP database to identify the serving registrar in the MC 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 [9].

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 MC 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 MC 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 [9].

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 MC service provider provides the SIP core, the SIP database may be provided by the MC 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;
- MC service 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 MC service 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 MC services based on MC 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 MC service use or a registrar in a secure location) or a registrar within the MC 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 MC 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 MC service server(s).

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 a proxy for hypertext transactions between the HTTP client and one or more HTTP servers. The HTTP proxy terminates a TLS session on HTTP-1 with the HTTP client of the MC service UE allowing the HTTP client to establish a single TLS session for hypertext transactions with multiple HTTP servers that are reachable by the HTTP proxy.

The HTTP proxy is not used as part of CSC-1 interface. CSC-1 is a direct HTTP interface between the IdM client in the UE and the IdM server as specified in 3GPP TS 33.179 [20].

According to 3GPP TS 33.179 [20], either an HTTP proxy or a direct HTTP interface is used between the key management server and the key management client in the UE for CSC-8.

The HTTP proxy shall be in the same trust domain as the HTTP clients and HTTP servers that are located within a MC service provider's network. There can be multiple instances of an HTTP proxy e.g. one per trust domain.

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 MC service 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 [6].

7.5.2 Application plane

7.5.2.1 General

The reference points for the application plane of an MC service are described in the following subclauses.

7.5.2.2 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 MC service 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 [20].

7.5.2.3 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 MC service signalling for MC service data management of the MC 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.

7.5.2.4 Reference point CSC-3 (between the MC service server and the group management server)

The CSC-3 reference point, which exists between the MC service server and the group management server, provides for the MC service server to obtain group information corresponding to the MC service. 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.

7.5.2.5 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 MC services while the MC service client is on-network.

The CSC-4 reference point supports:

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

7.5.2.6 Reference point CSC-5 (between the MC service server and the configuration management server)

The CSC-5 reference point, which exists between the MC service server and the configuration management server, provides for the MC service server to obtain non-group MC 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.

7.5.2.7 Reference point CSC-7 (between the group management servers)

The CSC-7 reference point, which exists between group management servers, allows group management servers to handle group management related signalling in multiple MC service 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.

7.5.2.8 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 [20].

7.5.2.9 Reference point CSC-9 (between the key management server and the MC service server)

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

CSC-9 is specified in 3GPP TS 33.179 [20].

7.5.2.10 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.

CSC-10 is specified in 3GPP TS 33.179 [20].

7.5.2.11 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 MC services while the MC service 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.

7.5.2.12 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 MC service application signalling for data management of the MC 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.

7.5.2.13 Reference point CSC-13 (between the configuration management server and the MC service user database)

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

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

7.5.2.14 Reference point CSC-14 (between the location management client and the location management server)

The CSC-14 reference point, which exists between the location management client and the location management server, is used by the location management server to receive location information report from location management client.

The CSC-14 reference point uses SIP-1 and SIP-2 reference points for transport and routing of subscription/notification related signalling. The CSC-14 reference point uses the HTTP-1 and HTTP-2 reference points for transport and routing of non-subscription/notification related signalling.

7.5.2.15 Reference point CSC-15 (between the location management server and the MC service server)

The CSC-15 reference point, which exists between the location management server and the MC service server, is used by the MC service server to request and receive location information from location management server.

The CSC-15 reference point uses SIP-1 and SIP-2 reference points for transport and routing of subscription/notification related signalling. The CSC-15 reference point uses the HTTP-1 and HTTP-2 reference points for transport and routing of non-subscription/notification related signalling.

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 MC service, shall use the Gm reference point as defined in 3GPP TS 23.002 [6] (with necessary enhancements to support MC service requirements and profiled to meet the minimum requirements for support of MC service). The SIP-1 reference point fulfils the requirements of the GC1 reference point specified in 3GPP TS 23.468 [18]. The SIP-1 reference point is used for:

- SIP registration;
- authentication and security to the service layer;
- event subscription and event notification;
- communication of the TMGI for multicast operation;
- overload control;
- 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 MC service, shall use the ISC and Ma reference points as defined in 3GPP TS 23.002 [6]. The SIP-2 reference point is used for:

- notification to the MC service server(s) of SIP registration by the MC service UE;
- authentication and security to the service layer;
- event subscription and event notification;
- communication of the TMGI for multicast operation;
- 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 MC service, shall use the Mm and ICi reference points as defined in 3GPP TS 23.002 [6]. The SIP-3 reference point is used for:

- event subscription and event notification;
- 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 MC service UE and the HTTP proxy, the HTTP-1 reference point shall use the Ut reference point as defined in 3GPP TS 23.002 [6] (with necessary enhancements to support specific MC service 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 [6].

In some deployment scenarios the registrar and SIP database are located in the MC 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 MC service 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 MC service ID may be the same. The MC ID uniquely identifies the MC service 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 [20].

8.1.2 MC service user identity (MC service ID)

The MC service user identity is also known as the MC service ID. The MC service ID is a globally unique identifier within the MC service that represents the MC service user. The MC service ID identifies an MC service user. The MC service ID may also identify one or more MC service user profiles for the user at the application layer.

There are attributes associated with the MC service ID configured in the MC service that relate to the human user of the MC service. Typically this information identifies the MC service user, by name or role, may also identify a user's organization or agency, and may also identify MC service user’s service subscription to one or more MC services. Such attributes associated with an MC service ID can be used by the MC service server to make authorization decisions about the MC service granted to the user. For example, if the MC service user is subscribed to MCPTT service, 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 MC service ID shall be a URI. The MC service ID uniquely identifies an MC service user in an MC system. The MC service ID indicates the MC system where the MC service ID is defined.

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

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

8.1.3 MC service group identity (MC service group ID)

8.1.3.1 General

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

The MC service group ID identifies an MC service group in an MC system. It indicates the MC system where the MC service group is defined. It indicates the MC service server within the MC system where the group is defined as described in subclause 8.3.2.

The MC service group ID is used as follows:

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

b) By the MC service client to address the MC service group.

The MC service group ID shall be a URI.

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

8.1.3.2 MC service group ID management (off-network operation)

In off-network operation, an MC service group ID is used for identifying the MC service group while off-network. The MC service group ID should be resolved to the ProSe Group IP multicast address and ProSe Layer-2 Group ID for the group communication. The MC service UE is able to make one or more MC service communications (as per the group configuration) with other member UEs whose users are of the same MC service group ID over ProSe direct communications based on ProSe Layer-2 Group ID and ProSe Group IP multicast address, and utilising IPv4 or IPv6 as indicated by policy, as described in 3GPP TS 23.303 [14].

Figure 8.1.3.2-1 illustrates how the MC service 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 MC service 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 [14], or be delivered from an application server. Mapping information is provisioned from group management server for online configuration, and provisioned from configuration management server for 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.

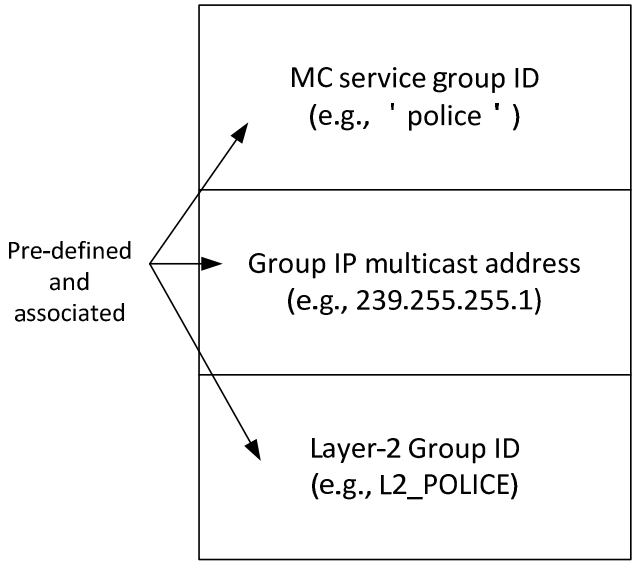

Figure 8.1.3.2-1: MC service group ID management in off-network operation

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 [9].

All SIP signalling messages sent by a signalling user agent to an MC service 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 [9].

NOTE 1: The relationship between the private user identity and public user identity is defined in 3GPP TS 23.228 [9].

The public user identities do not necessarily contain any application-level attributes of MC services (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 MC service are part of the same trust domain, public user identities may be provided by the MC service provider or the PLMN operator. When the SIP core and the MC service are part of the different trust domains, public user identities may be provided by the PLMN operator.

NOTE 2: The MC 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 MC service UEs when a user logging on from multiple devices or multiple users sharing the same device is supported per 3GPP TS 23.228 [9].

Public service identity is used as the identifier to route SIP signalling for the MC system. The public service identity fulfils the same functions as PSI defined in 3GPP TS 23.228 [9].

8.3 Relationship between identities in different planes

8.3.1 Relationship between MC service ID and public user identity

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

- An MC service ID may be mapped to one or more public user identities (e.g. multiple UEs, shared UE, multiple MC services);
- A public user identity may be mapped to one or more MC service IDs (e.g. UE-to-network relay); and
- An MC service 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 MC service server manages the mapping between MC service IDs and public user identities.

The MC service server manages the mapping between MC service IDs and public GRUUs.

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

The public user identity does not necessarily identify the MC service user at the SIP signalling control plane. When the MC 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 MC service user at the application plane.

8.3.2 Relationship between MC service group ID and public service identity

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

When the MC 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 MC service group ID at the application plane.

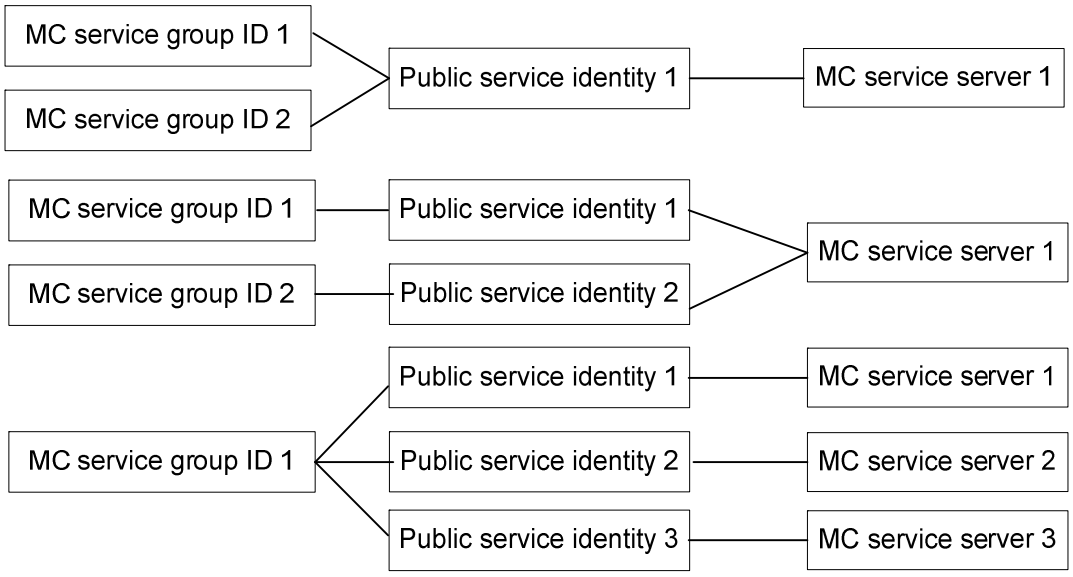

Figure 8.3.2-1: The relationship of MC service group IDs, PSIs and MC service servers

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 MC system solution, where the MC system provides one or more MC services via a single PLMN.

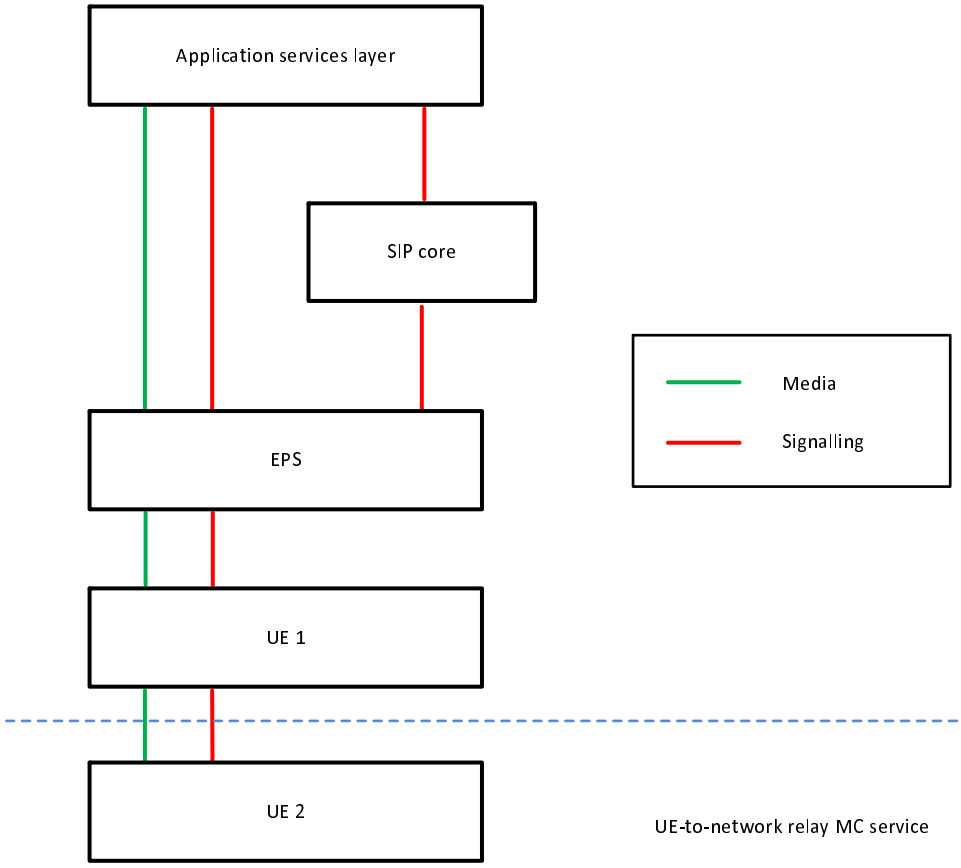

Figure 9.2.1.1-1: On-network architectural model

9.2.1.2 Application services layer

9.2.1.2.1 Overview

The application services layer includes application functions of one or more MC services 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, an identity management server as described in subclause 7.4.2.2.6 and a key management server as described in subclause 7.4.2.2.8; 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 MC services

MC services are composed of the following functional entities:

- an MC service server as described in subclause 7.4.2.3.2 with relevant application functions of the corresponding MC service defined in the corresponding MC service TS.

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:

- an MC service UE in on-network mode supporting bearer services and application(s) related to one or more MC service;
- an MC service UE that acts as ProSe UE-to-network relay; or
- both of the above.

When acting as an MC service UE in on-network mode supporting bearer services and application(s) related to one or more MC services, UE 1 is composed of the same functional entities as for UE 2, as described in subclause 9.2.1.6, without the support of ProSe capabilities.

9.2.1.6 UE 2

UE 2 is a device using ProSe UE-to-network relay, and supporting application(s) related to one or more MC services. 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, an identity management client as described in subclause 7.4.2.2.5 and a key management client as described in subclause 7.4.2.2.7;
- for MC services, MC service clients as described in subclause 7.4.2.3.1 with relevant application functions of the corresponding MC service defined in the corresponding MC service TS; and
- 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.

9.2.2 Deployment scenarios

9.2.2.1 Administration of MC service, SIP core and EPS

9.2.2.1.1 General

This subclause describes five different deployment scenarios in which different administration of MC 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 MC service provider may own some RAN components within the EPS even when the EPS is administered by the PLMN operator, and the MC service UE may be owned by an organisation that is independent from PLMN and MC 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.

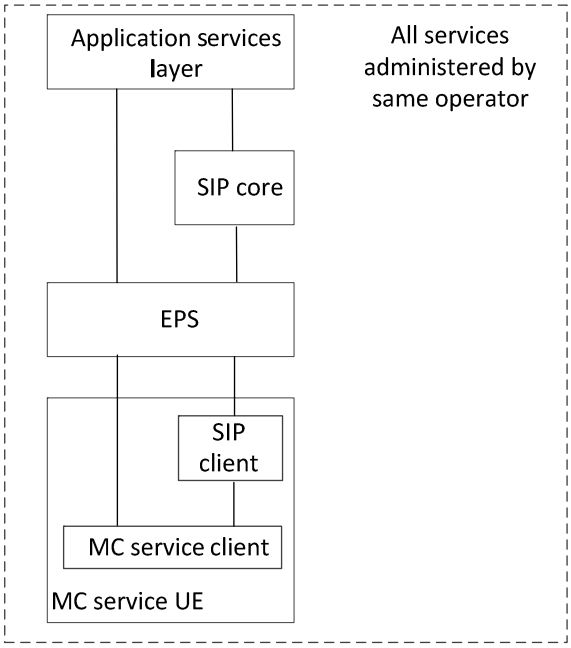

Figure 9.2.2.1.2-1: Common administration of all services by one operator

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 MC service provider separate from SIP core and EPS

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

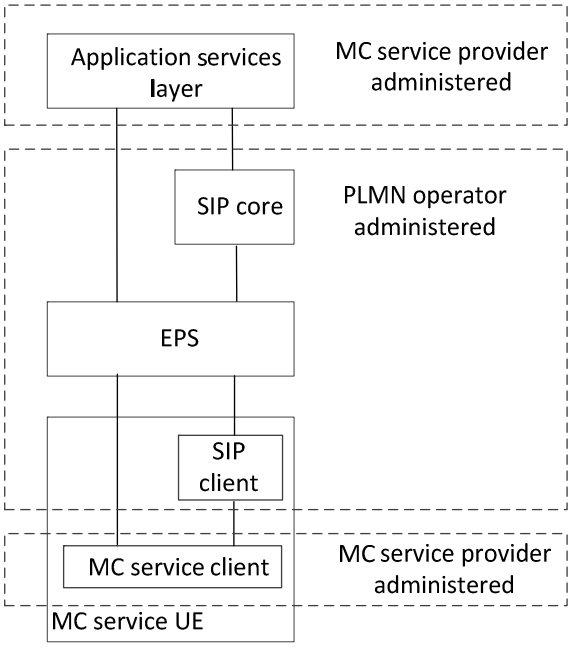

Figure 9.2.2.1.3-1: MC service provider administers MC service separately from SIP core and EPS

The MC 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 MC 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 MC service provider administers SIP core, separate from EPS

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

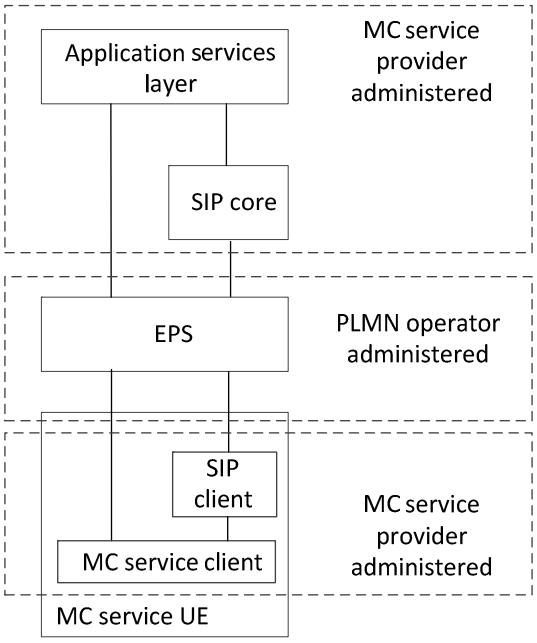

Figure 9.2.2.1.4-1: MC service provider provision of SIP core, separate domain from EPS

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

layer from the SIP core. However the MC service provider may require that identities and other sensitive information between SIP core and SIP client in the MC service 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 MC 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 MC service provider, but the SIP core registrar finder and proxy is administered by the PLMN operator.

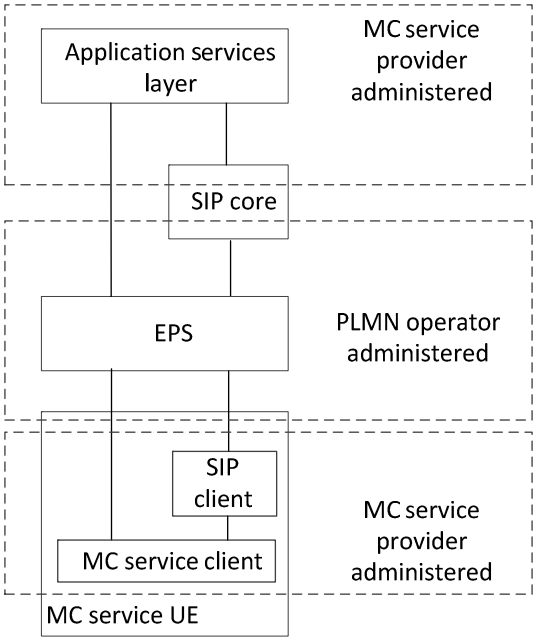

Figure 9.2.2.1.5-1: MC service provider partial provision of SIP core, separate domain from EPS

The MC 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 MC service provider

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

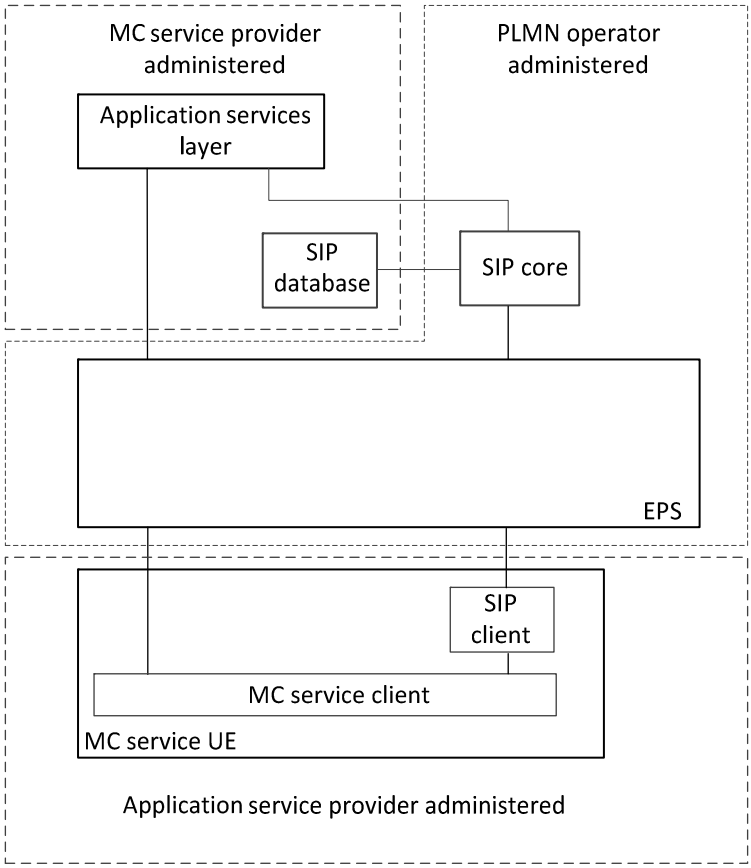

Figure 9.2.2.1.6-1: MC service provider provides identities to PLMN operator SIP core

The MC 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 MC 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 MC service provider's SIP 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 MC service 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 MC service user database and SIP database, including collocation with the HSS.

The MC service user database may be combined with an HSS in some deployment scenarios (e.g. when the MC service provider and the PLMN operator are part of the same trust domain).

The MC service user database may be a user data repository (UDR) in deployment scenarios when the UDC architecture is applied (see 3GPP TS 23.335 [15]), in that case the MC service server and the configuration management server are assumed to be application front-ends and the Ud interface is used to access data from the repository.

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

NOTE 2: The MC service user database and the MC service server are always deployed in the same network i.e. both in the PLMN operator's network or both in the MC service provider's network.

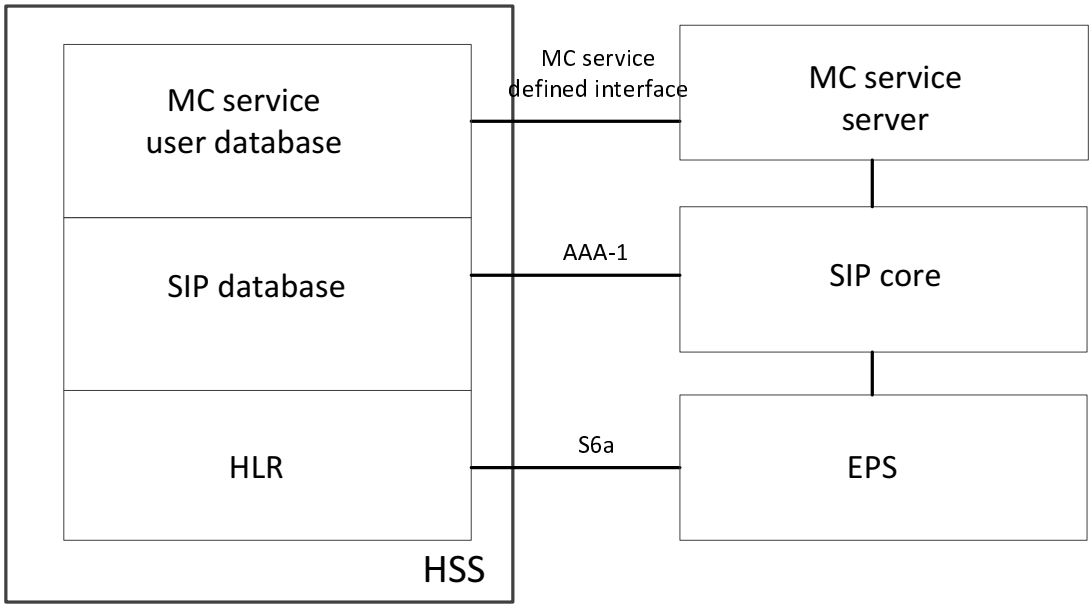

Figure 9.2.2.2-1: Collocation of MC service user database and SIP database with HSS

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

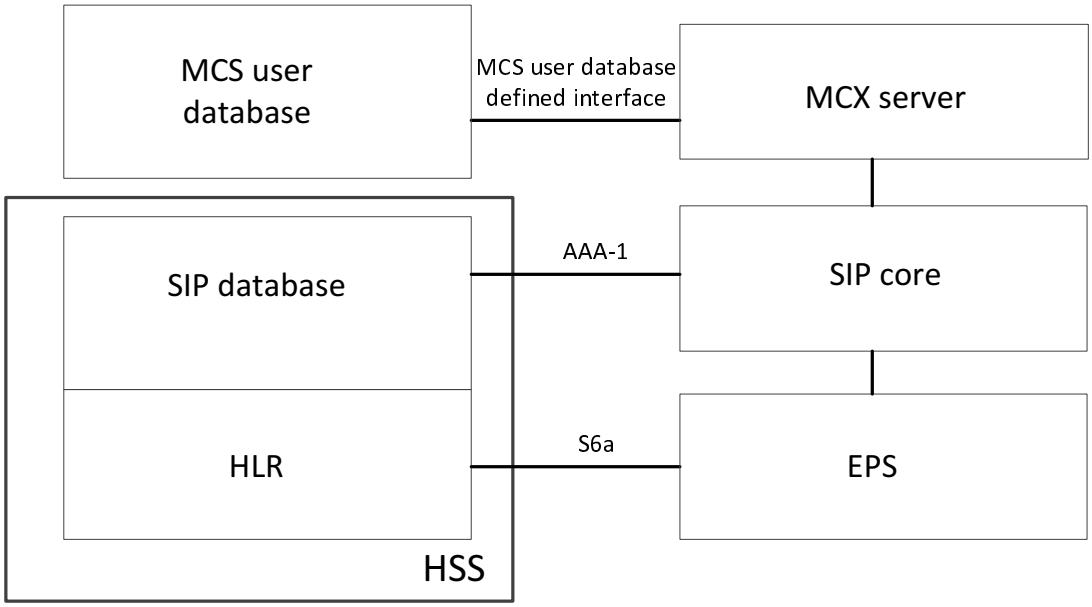

Figure 9.2.2.2-2: Shared PLMN operator and MC service provider based deployment of MC service - SIP database collocated with HSS with separate MC service user database

The MC service user database depicted in figure 9.2.2.2-2 can be deployed in the PLMN operator's network or the MC 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 MC service user database i.e. PLMN operator's network or the MC service provider's network.

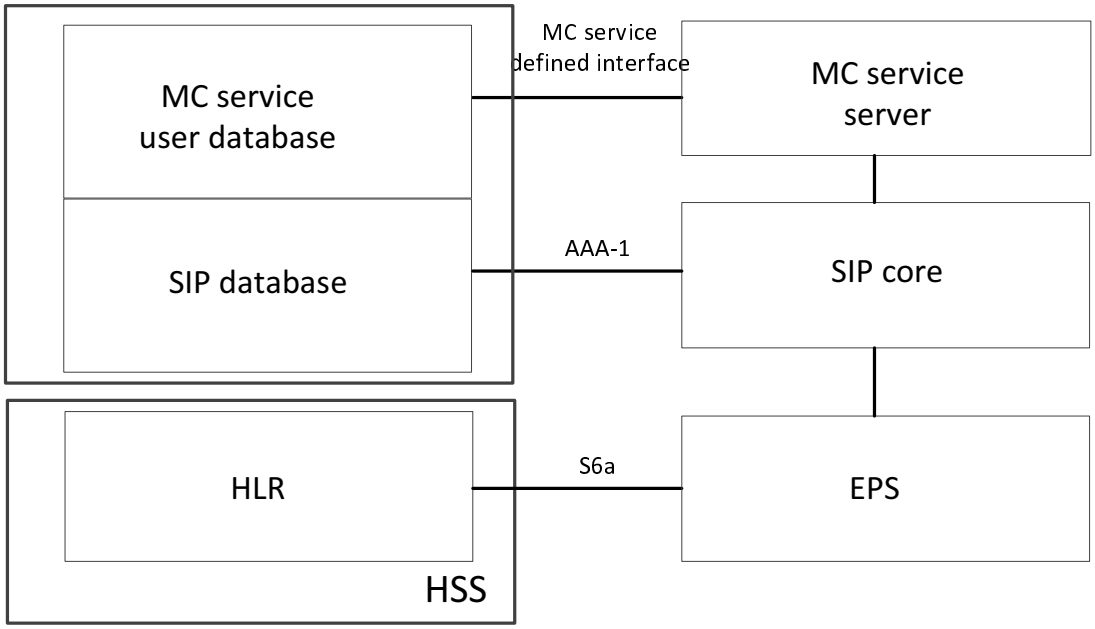

Figure 9.2.2.2-3: Shared PLMN operator and MC service provider based deployment of MC service - MC service user database and SIP database deployed together, with separate HSS

The MC service user database and SIP database depicted in figure 9.2.2.2-3 can be deployed in the PLMN operator's network or the MC 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 MC service user database i.e. PLMN operator's network or the MC service provider's network.

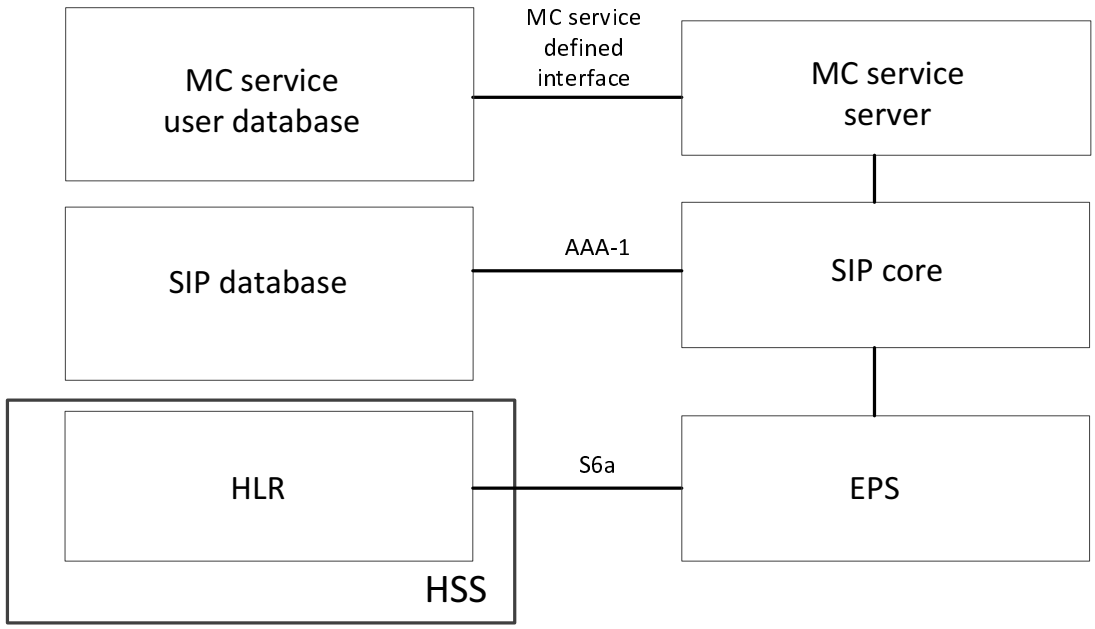

Figure 9.2.2.2-4: Shared PLMN operator and MC service provider based deployment of MC service - separate HSS, MC service user database and SIP database

Each of the MC service 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 MC service provider's network.

9.2.2.3 Control of bearers by SIP core and MC service 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 MC service 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.

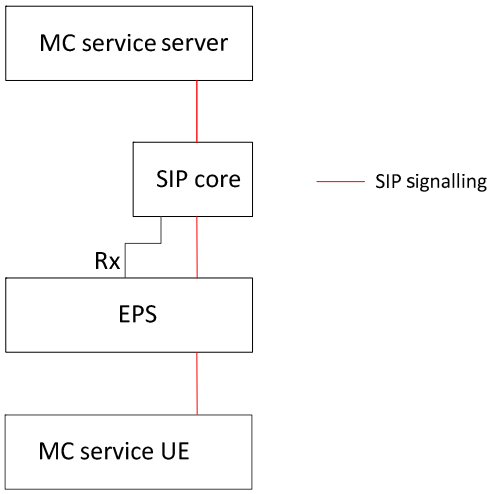

Figure 9.2.2.3.2-1: Bearer control by SIP core

9.2.2.3.3 Control of bearers by MC service server

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

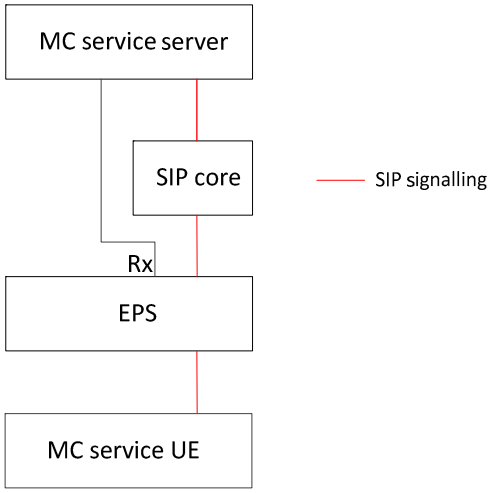

Figure 9.2.2.3.3-1: Bearer control by MC service server

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 MC system solution for inter-UE communication, where no relay function is used.

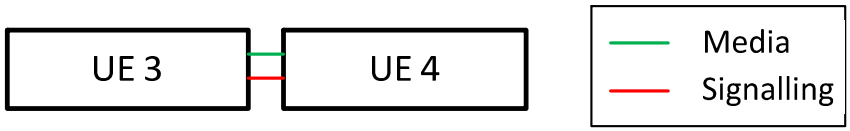

Figure 9.3.1-1: Off-network architectural model for inter-UE communication where no relay function is used

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

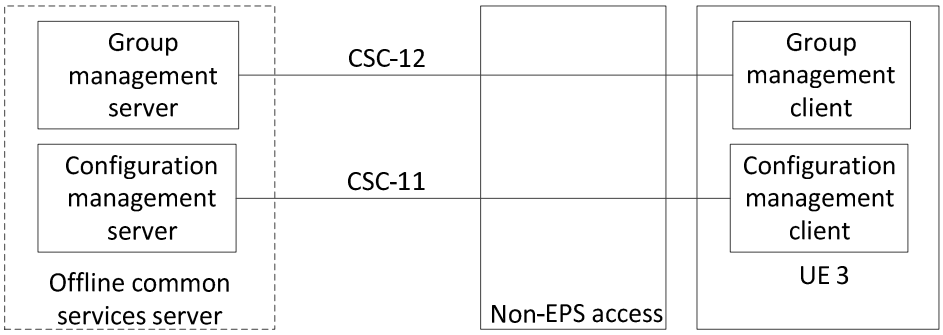

Figure 9.3.1-2: Off-network architectural model for configuration management and group management

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 or WLAN.

The offline common services server could be the same entity (or set of entities) as the common services core. In this case the configuration management server shall not configure to the same user on the same UE, with parameters provisioned by offline and online configuration simultaneously. The configuration management server shall not configure to the same user on the same UE for the same parameters by using CSC-11 and CSC-4 reference points simultaneously.

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 MC service, and is composed of the following functional entities:

- for MC services, MC service clients as described in subclause 7.4.2.3.1 with relevant application functions of the specific MC service defined in the corresponding MC service TS;
- 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; and
- for group management, a group management client as described in subclause 7.4.2.2.3.

9.3.3 UE 4

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

9.3.4 Offline common services server

The offline common services server supports configuration applications related to MC 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 [17]; or
- IMS-level roaming as defined in 3GPP TS 23.228 [9].

10 Procedures and information flows

10.1 MC service configuration

10.1.1 General

Depicted in figure 10.1.1-1 is a MC service configuration time sequence of the data related to specific MC service, representing the general lifecycle of MC service UE using an MC service.

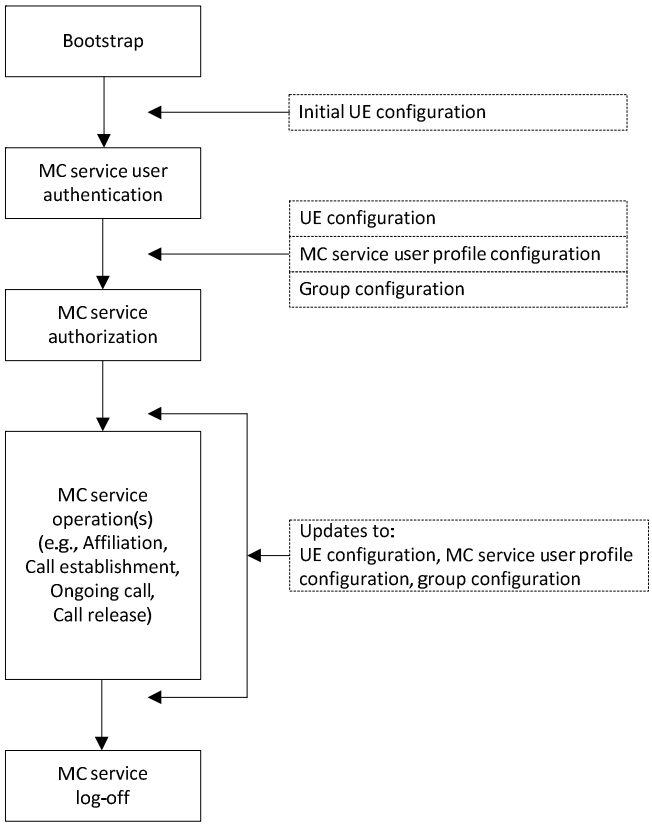

Figure 10.1.1-1 MC service UE configuration time sequence and associated configuration data

The MC service UE is provided with initial UE configuration via a bootstrap procedure that provides the MC service UE's clients (e.g. MC service client, group management client, configuration management client, identity management client, key management client) with critical information needed to connect to the MC system. This includes PDN connection information corresponding to the configured MC services on the MC service UE (see "EPS bearer considerations" in the 3GPP TS 23.379 [16]) and on-network server identity information for all application plane servers with which the MC service UE needs to interact. See annex A.6 for more information.

The MC service UE is provided with UE configuration, MC service user profile configuration and group configuration via online configuration. While the MC service UE is using the MC service it may receive online configuration updates. If the MC service user profile configuration contains multiple MC service user profiles for an authenticated MC service user, then the MC service client and MC service server set the active MC service user profile to the configured pre-selected MC service user profile at MC service authorization (which can be updated by the MC service user using the procedure specified in subclause 10.1.4.6). The active MC service user profile can be changed by the MC service user to a different MC service user profile during MC service service (see MC service TSs).

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

Editor's note: Providing MC services to an MC service UE with an unauthenticated MC service user is FFS.

10.1.2 Information flows for MC service 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
MC service group ID	M	MC service group ID of the group
MC service group configuration data	M	MC service 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
MC service group ID	M	MC service group ID of the group
Result	M	Indicates the success or failure for the result

10.1.2.3 Get group configuration request

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

Table 10.1.2.3-1: Get group configuration request

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
MC service group information reference	M	Reference to configuration data for the MC service group
MC services requested (see NOTE)	O	Service(s) for which group configuration is requested; one or more of MCPTT, MCVideo, MCData
NOTE: If 'MC services requested' is not present, group configuration is requested for all services defined for the MC service group		

10.1.2.4 Get group configuration response

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

Table 10.1.2.4-1: Get group configuration response

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
MC service group configuration data	M	MC service group configuration data

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
MC service group ID	M	MC service group ID of the group
MC services requested (see NOTE)	O	Service(s) for which group configuration is requested; one or more of MCPTT, MCVideo, MCData
NOTE: If 'MC services requested' is not present, group configuration is requested for all services defined for the MC service 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
MC service group ID	M	MC service group ID of the group
Result	M	Indicates the success or failure for the result

10.1.2.7 Notify group configuration request

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

Table 10.1.2.7-1: Notify group configuration request

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
MC service group information reference (NOTE)	O	Reference to information stored relating to the MC service group
Group related key material (NOTE)	O	Key material for use with the MC service group
NOTE: At least one of these information elements shall be present.		

10.1.2.8 Notify group configuration response

Table 10.1.2.8-1 describes the information flow notify group configuration response from the group management client to the group management server.

Table 10.1.2.8-1: Notify group configuration response

Information element	Status	Description
MC service group ID	M	MC service group ID of the group
Result	M	Indicates the success or failure for the result

10.1.3 MC service UE configuration data

10.1.3.1 General

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

10.1.3.2 Procedures

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

Pre-conditions:

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

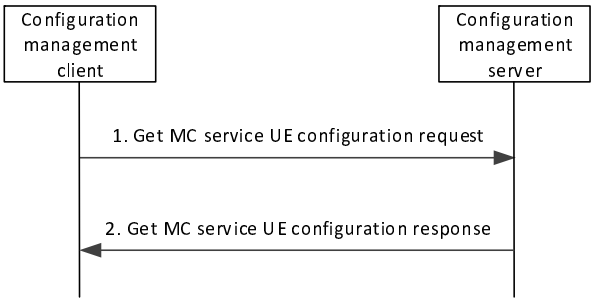

Figure 10.1.3.2-1: MC service UE obtains the configuration data

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

10.1.3.3 Structure of UE configuration data

For a MC service, the MC service UE configuration data is listed in the corresponding MC service TS.

10.1.4 MC service user profile

10.1.4.1 General

An MC service user is identified by an MC service ID. An MC service ID is associated with at least one MC service user profile and can be associated with multiple MC service user profiles (identified by an index and optionally a profile name). This is depicted in figure 10.1.4.1-1.

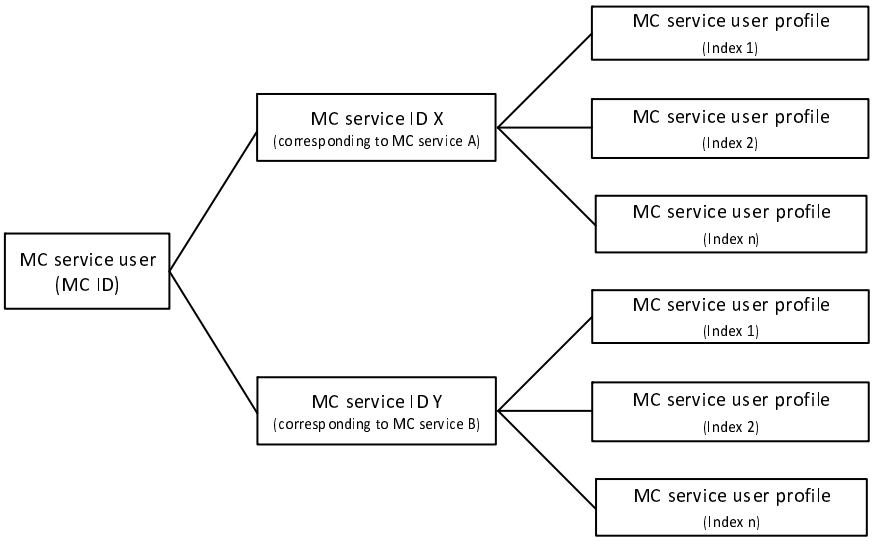

Figure 10.1.4.1-1: The relationship of MC service user, MC service IDs, MC service user profile and MC services

For an MC service user there can be multiple MC service IDs with the constraint that only one MC service ID exists for a given MC service for that MC service user (e.g. MC service ID X may correspond to MCPTT service and MC service

ID Y may correspond to MCVideo service). When the MC service provider requires to support a single MC service ID for all MC services, the value of the multiple MC service IDs is the same (e.g. value of MC service ID X is same as MC service ID Y).

In the case where a single MC service ID is configured for a MC service user for authorized access to multiple MC services, the MC service UE and MC service server shall include the indication of the specific MC service during the communication.

For the same MC service user there can be different MC service user profiles active on different MC service UEs or different MC service user profiles active on the same MC service UE at different times. Only one MC service user profile per MC service client is active at a time.

All MC service user profiles associated with an MC service user are stored in the MC service user database. Different parts of the MC service user profile are provisioned by the Mission Critical Organization, by the MC service provider and by the MC service user, respectively.

MC service user profile information is downloaded to the MC service UE. The MC service user profile provisioning in the UE is initiated by the configuration management client (e.g. upon MC service user authentication or on reconnect to the MC service), or initiated by the configuration management server (e.g. due to role change or organization change). MC service user profile configuration may include more than one information exchange e.g. the configuration management server may provide the MC service UE with a list of some or all enabled MC service user profiles to allow the MC service user to select one (where the list may contain a subset of the MC service user profile information sufficient for the MC service user to distinguish which MC service user profile to select).

10.1.4.2 Information flows for MC service user profile

10.1.4.2.1 Get MC service user profile request

Table 10.1.4.2.1-1 describes the information flow get MC service user profile request from the configuration management client to the configuration management server.

Table 10.1.4.2.1-1: Get MC service user profile request

Information element	Status	Description
MC service ID	M	The MC service ID of the MC service user.

10.1.4.2.2 Get MC service user profile response

Table 10.1.4.2.2-1 describes the information flow get MC service user profile response from the configuration management server to the configuration management client.

Table 10.1.4.2.2-1: Get MC service user profile response

Information element	Status	Description
MC service user profile data	M	One or more MC service user profiles (identified as specified in subclause 10.1.4.1) associated with the MC service ID provided in the associated get MC service user profile request.

10.1.4.2.3 Notification for MC service user profile data update

Table 10.1.4.2.3-1 describes the information flow notification for MC service user profile data update from the configuration management server to the configuration management client.

Table 10.1.4.2.3-1: Notification for MC service user profile data update

Information element	Status	Description
Pointer to modified MC service user profile data.	M	Pointer to the modified MC service user profile data.

10.1.4.2.4 Get updated MC service user profile data request

Table 10.1.4.2.4-1 describes the information flow get updated MC service user profile data request from the configuration management client to the configuration management server.

Table 10.1.4.2.4-1: Get updated MC service user profile data request

Information element	Status	Description
MC service ID	M	The MC service ID of the originating MC service user.
Pointer to modified MC service user profile data.	M	Pointer to the modified MC service user profile data.

10.1.4.2.5 Get updated MC service user profile data response

Table 10.1.4.2.5-1 describes the information flow get updated MC service user profile data response from the configuration management server to the configuration management client.

Table 10.1.4.2.5-1: Get updated MC service user profile data response

Information element	Status	Description
Updated MC service user profile data	M	MC service user profile data that has been modified.

10.1.4.2.6 Update MC service user profile data request

Table 10.1.4.2.6-1 describes the information flow update MC service user profile data request from the configuration management client to the configuration management server.

Table 10.1.4.2.6-1: Update MC service user profile data request

Information element	Status	Description
MC service ID	M	The MC service ID of the originating MC service user.
Updated MC service user profile data	M	The contents of the user profile data to be updated.

10.1.4.2.7 Update MC service user profile data response

Table 10.1.4.2.7-1 describes the information flow update MC service user profile data response from the configuration management server to the configuration management client.

Table 10.1.4.2.7-1: Update MC service user profile data response

Information element	Status	Description
Result	M	Indicates the success or failure

10.1.4.2.8 Update pre-selected MC service user profile request

Table 10.1.4.2.8-1 describes the information flow update pre-selected MC service user profile request from the configuration management client to the configuration management server.

Table 10.1.4.2.8-1: Update pre-selected MC service user profile request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator.
MC service user profile index	M	The MC service user profile index of the MC service user profile that is to be pre-selected by the MC service server at MC service user authentication.

10.1.4.2.9 Update pre-selected MC service user profile response

Table 10.1.4.2.9-1 describes the information flow update pre-selected MC service user profile response from the configuration management server to the configuration management client.

Table 10.1.4.2.9-1: Update pre-selected MC service user profile response

Information element	Status	Description
Result	M	Indicates the success or failure.

10.1.4.2.10 Update selected MC service user profile request

Table 10.1.4.2.10-1 describes the information flow update selected MC service user profile request from the MC service client to the MC service server and is used by the following MC services:

- MCPTT (as specified in 3GPP TS 23.379 [16]);
- MCVideo (as specified in 3GPP TS 23.281 [12]); and
- MCData (as specified in 3GPP TS 23.282 [13]).

Table 10.1.4.2.10-1: Update selected MC service user profile request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator.
MC service user profile index	M	The MC service user profile index of the selected MC service user profile.

10.1.4.2.11 Update selected MC service user profile response

Table 10.1.4.2.11-1 describes the information flow update selected MC service user profile response from the MC service server to the MC service client and is used by the following MC services:

- MCPTT (as specified in 3GPP TS 23.379 [16]);
- MCVideo (as specified in 3GPP TS 23.281 [12]); and
- MCData (as specified in 3GPP TS 23.282 [13]).

Table 10.1.4.2.11-1: Update selected MC service user profile response

Information element	Status	Description
Result	M	Indicates the success or failure.

10.1.4.3 MC service user obtains the MC service user profile(s) from the network

The procedure for the MC service user obtaining the MC service user profiles is illustrated in figure 10.1.4.3-1.

Pre-conditions:

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

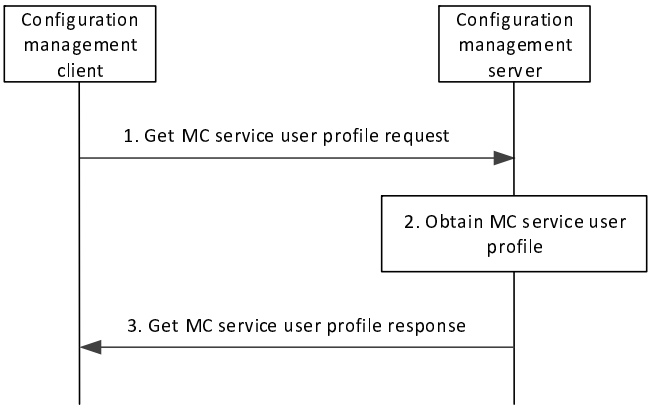

Figure 10.1.4.3-1: MC service user obtains the MC service user profile(s) from the network

1. The configuration management client sends a get MC service user profile request message to the configuration management server, which includes the MC service ID.
2. The configuration management server obtains the MC service user profile information.
3. The configuration management server sends get MC service user profile response message to the configuration management client. When a download is necessary, this message includes all MC service user profiles that are associated with the MC service ID.

10.1.4.4 MC service user receives updated MC service user profile data from the network

The procedure for MC service user obtaining updated MC service user profile data (see 3GPP TS 23.379 [16]) that is initiated by the network is illustrated in figure 10.1.4.4-1.

Pre-conditions:

- The MC service user has performed user authentication in identity management server.
- The MC service UE has secure access to the configuration management server.
- The MC service UE has already obtained one or more MC service user profiles.
- The configuration management server has access to the MC service user profile(s) associated with the MC service ID of the MC service user.

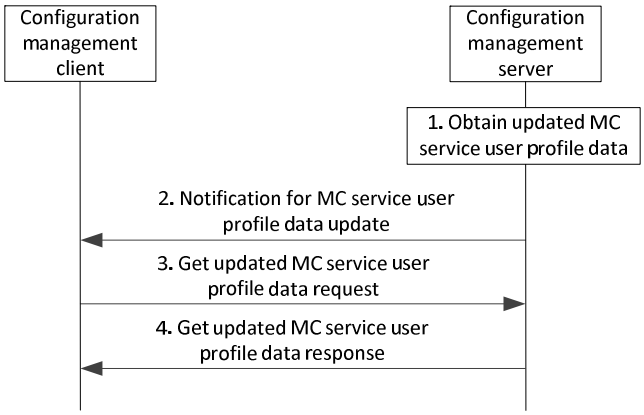

Figure 10.1.4.4-1: MC service user receives updated MC service user profile data from the network

1. The configuration management server obtains updated MC service user profile data.
2. The configuration management server sends a notification for MC service user profile data update to the configuration management client.
3. The configuration management client sends get updated MC service user profile data request to the configuration management server, which includes the MC service ID.
4. The configuration management server sends get updated MC service user profile data response to the configuration management client which includes the updated MC service user profile data requested in step 3.

NOTE: The updated MC service user profile data could be for a specific MC service user profile, a specific parameter in an MC service user profile, a set of MC service user profiles, or all the MC service user profiles for the MC service ID. MC service user profile data is defined per MC service. E.g. the MC service user profile data related to MCPTT is defined in 3GPP TS 23.379 [16].

10.1.4.5 MC service user updates MC service user profile data to the network

The procedure for MC service user updating the MC service user profile data (see 3GPP TS 23.379 [16]) is illustrated in figure 10.1.4.5-1.

Pre-conditions:

- The MC service user has performed user authentication in identity management server.
- The MC service UE has secure access to the configuration management server.
- The MC service UE has already obtained one or more MC service user profiles.

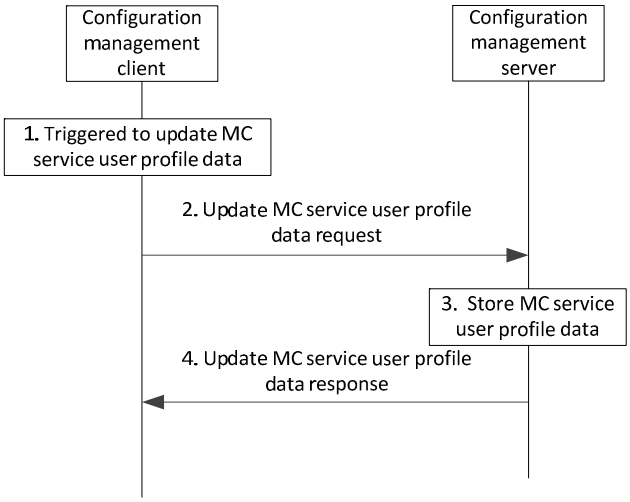

Figure 10.1.4.5-1: MC service user updates MC service user profile data to the network

1. The configuration management client is triggered (e.g. by user interaction operation) to update the MC service user profile data on the configuration management server.
2. The configuration management client sends update MC service user profile data request to the configuration management server, which includes the MC service user profile data to be updated.
3. The configuration management server stores the received MC service user profile data.
4. The configuration management server sends update MC service user profile data response to the configuration management client to confirm the MC service user profile data update is complete.

NOTE: The updated MC service user profile data could be for a specific MC service user profile, a specific parameter in an MC service user profile, a set of MC service user profiles, or all the MC service user profiles for the MC service ID. MC service user profile data is defined per MC service. E.g. the MC service user profile data related to MCPTT is defined in 3GPP TS 23.379 [16].

10.1.4.6 Updating the pre-selected MC service user profile

The procedure for updating the pre-selected MC service user profile in the configuration for an MC service UE by the MC service user is illustrated in figure 10.1.4.6-1.

Pre-conditions:

- The MC service user has performed user authentication in identity management server.
- The MC service UE has secure access to the configuration management server.
- The MC service UE has already obtained one or more MC service user profiles.
- The configuration management client is triggered (e.g. by user interaction, by some automated means) to change the pre-selected MC service user profile.

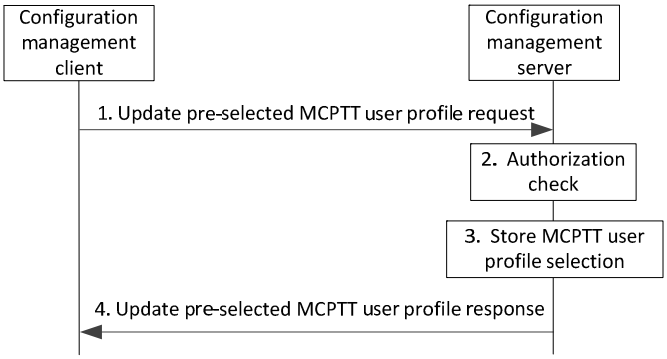

Figure 10.1.4.6-1: MC service user updates the pre-selected MC service user profile

1. The configuration management client sends update pre-selected MC service user profile request to the configuration management server, which includes the MC service user's MC service ID and an MC service user profile index that indicates which MC service user profile is to be pre-selected by the MC service server at next MC service authorization.
2. The configuration management server checks the authorization of the update pre-selected MC service user profile request.
3. The configuration management server stores the received pre-selected MC service user profile selection.
4. The configuration management server sends update pre-selected MC service user profile response to the configuration management client to confirm the pre-selected MC service user profile has been set.

NOTE: Steps 3 to 4 can occur in any order or in parallel.

For each update pre-selected MC service user profile request to the MC service user profile, the configuration management server determines whether the requested update is allowed prior to storing the configuration parameters and updating the MC service user database (via the CSC-13 reference point as specified in 3GPP TS 29.283 [19]).

After each update to the MC service user profile in the MC service user database, the MC service server receives the changes from the MC service user profile database via the corresponding MC service reference point defined between MC service server and the MC service user database, and all of the MC service UEs associated with the MC service user receive the updated MC service user profile as specified in subclause 10.1.4.4.

A change to the pre-selected MC service user profile while the MC service user is receiving MC service does not have any effect on the active MC service user profile, however, the change will be applied at the next MC service authorization.

Editor's note: Specifying pre-selected MC service user profile specific to each UE associated with an MC service user is FFS.

10.1.4.7 Updating the selected MC service user profile for an MC service

The procedure for updating the selected MC service user profile within a single MC service for an MC service UE by the MC service user whilst the MC service user is receiving that MC service service is illustrated in figure 10.1.4.7-1. This procedure is used by the following MC services:

- MCPTT (as specified in 3GPP TS 23.379 [16]);
- MCVideo (as specified in 3GPP TS 23.281 [12]); and
- MCData (as specified in 3GPP TS 23.282 [13]).

Pre-conditions:

- For the MC service (see list above) for which the selected MC service user profile is to be updated:
  - The MC service user has performed user authentication in the identity management server.
  - The MC service UE has secure access to the MC service server.
  - The MC service UE has already obtained multiple MC service user profiles.
  - The MC service UE has performed MC service authorization.
  - The MC service client is triggered (e.g. by user interaction, by some automated means) to select a particular MC service user profile as active.

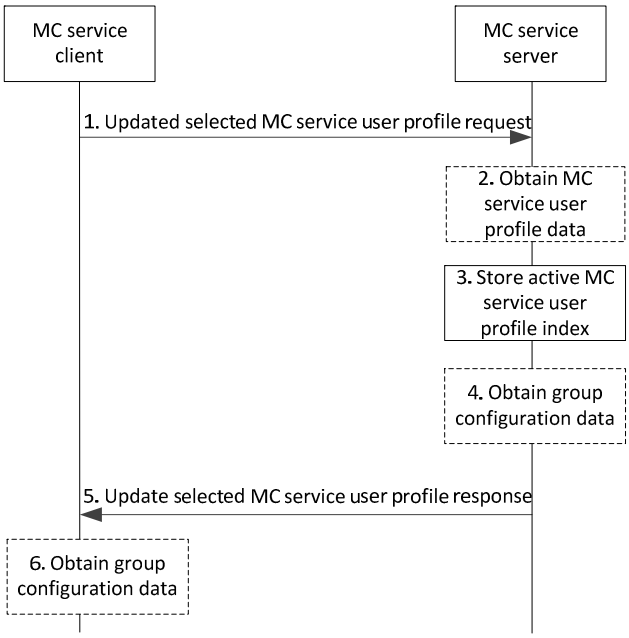

Figure 10.1.4.7-1: MC service user updates the selected MC service user profile

1. MC service client sends update selected MC service user profile request to the MC service server, which includes the MC service user's MC service ID and an MC service user profile index that indicates which MC service user profile is selected to be currently active for MC service client.
2. If the MPCTT server does not have stored the MC service user profile data for the MC service user, then the MC service server obtains the MC service user profile data.
3. The MC service server stores the selected MC service user profile index for the MC service client.

NOTE 1: Different MC service user profiles can be active for different MC service clients of the same MC service user.

4. If the MC service server does not have stored the group configuration data for the selected MC service user profile then the MC service server obtains group configuration data according to the selected MC service user profile (see subclause 10.1.5.2) and subscribes to updates of the group configuration data (see subclause 10.1.5.3).
5. The MC service server sends update selected MC service user profile response to the MC service client to confirm the active MC service user profile has been set.

NOTE 2: Steps 4 to 5 can occur in any order or in parallel.

6. If the MC service client does not have stored the group configuration data for the selected MC service user profile then the MC service client obtains group configuration data according to the successfully selected MC

service user profile (see subclauase 10.1.5.2) and subscribes to updates of the group configuration data (see subclause 10.1.5.3).

After each of the MC service server and the MC service UE have successfully negotiated a selected MC service user profile, then both the MC service server and the MC service UE, based upon the selected MC service user profile, clear any currently active service state from any previously selected or pre-selected MC service user profile data (including deaffiliating from relevant groups, disconnecting any MC service calls) and process the successfully negotiated selected MC service user profile data e.g. perform any needed affiliations.

10.1.5 MC service 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;

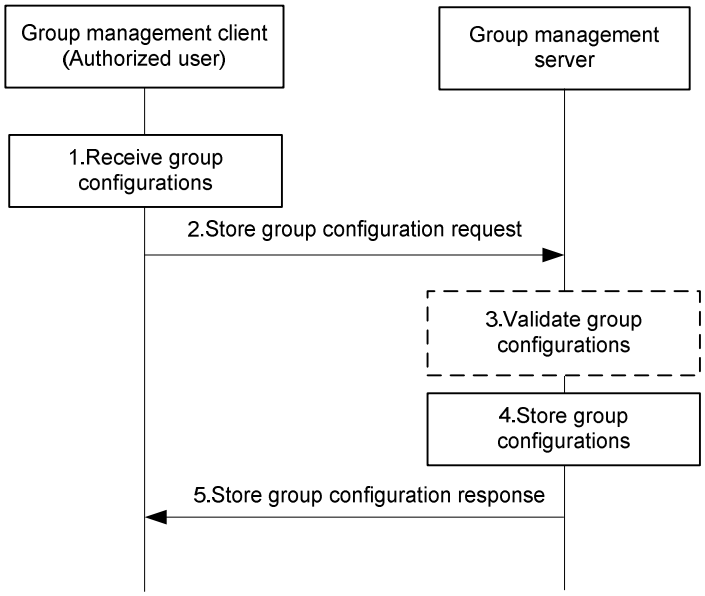

Figure 10.1.5.1-1: Store group configurations at group management server

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 Retrieve group configurations at the group management client

The procedure for retrieve group configurations at the group management client is described in figure 10.1.5.2-1. This procedure can be used following service authorisation when the configuration management client has received the list

of groups and the group management client needs to obtain the group configurations, or following a notification from the group management server that new group configuration information is available.

Pre-conditions:

- The group management server has received configuration data for groups, and has stored this configuration data;
- The MC service UE has registered for service and the group management client needs to download group configuration data applicable to the current user.

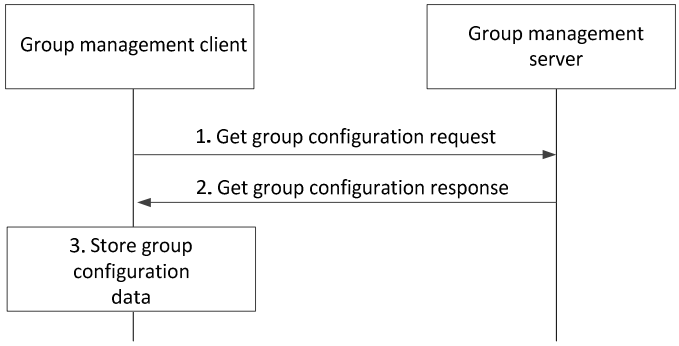

Figure 10.1.5.2-1: Retrieve group configurations at group management client

1. The group management client requests the group configuration data.
2. The group management server provides the group configuration data to the client.
3. The group management client stores the group configuration information.

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.

Pre-conditions:

- The group management server has some group configurations stored.

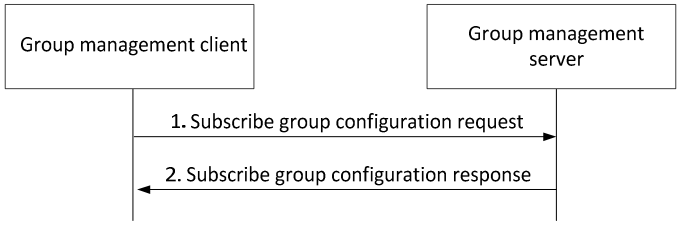

Figure 10.1.5.3-1: Subscription for group configurations

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.

The procedure for notification of group configuration data as described in figure 10.1.5.3-2 is used by the group management server to inform the group management client that new group configuration data is available. It can also be used by the group management server to provide new group related key material to the group management client.

Pre-conditions:

- The group management client has subscribed to the group configuration information

- The group management server has received and stored new group configuration information, or the group management server has generated and stored new key material, or both of these have occurred.

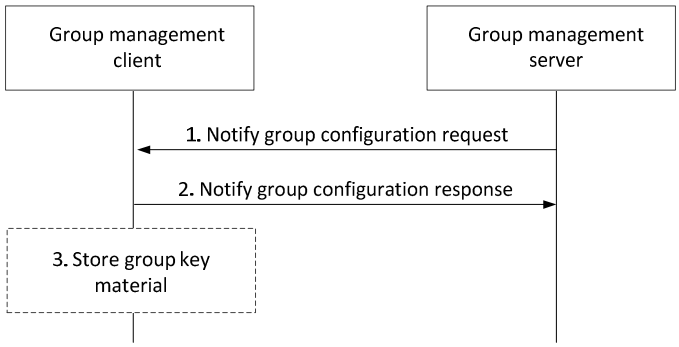

Figure 10.1.5.3-2: Notification of group configurations

1. The group management server provides the notification to the group management client, who previously subscribed for the group configuration information. Optionally, the notify group configuration request may contain group related key material for the group management client.
2. The group management client provides a notify group configuration response to the group management server.
3. If the group management server had provided group related key material to the group management client, the group management client stores the key material.

If the group management server has notified the group management client about new group configuration information through this procedure, the group management client may then follow the procedure described in subclause 10.1.5.2 in order to retrieve that group configuration information.

10.1.5.4 Structure of group configuration data

The group configuration data contains group configuration data common to all MC services and group configuration data specific to each MC service. All group configuration data is specified in Annex A.4 of the present document.

10.1.5.5 Dynamic data associated with a group

There may be dynamic data associated with a group. The following dynamic data is known to the MC service server and provided when requested:

Table 10.1.5.5-1: Dynamic data associated with a group

Parameter description
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.
Affiliation status of each MC service ID of the group corresponding to the MC service and the Contact URI(s) from which the user affiliated.
Contact URIs used for designation of the group e.g. aliases of group broadcast, group regroup group URIs.
Media description for group media, including transport and multiplexing information.
Group call ongoing.

10.2 Group management (on-network)

10.2.1 General

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

Group creation provides a dedicated MC service group to individual MC service users to enable the required communication for one or multiple MC services. This includes the normal group creation by administrators as well as user regrouping by authorized user/dispatcher.

For an MC service, group regrouping enables dispatchers or authorized users to temporarily combine several MC service groups.

NOTE 1: If an authorized MC service user wants to participate in a new group created by the authorized MC service user, then the authorized MC service user needs to have been included in the new group as a member and have affiliated to the new group.

NOTE 2: If an authorized MC service user wants to participate in a temporary group created by a group regroup operation performed by this authorized MC service user, then the authorized MC service user needs to have been an existing member of and affiliated to at least one of the constituent groups that was part of the associated group regroup operation and have affiliated to the new temporary group.

10.2.2 Information flows for group management

10.2.2.1 Group creation request

Table 10.2.2.1-1 describes the information flow group creation request from the group management client to the group management server.

Table 10.2.2.1-1: Group creation request

Information element	Status	Description
MC service ID list	M	List of MC service IDs that are part of the group to be created corresponding to the list of the configured services
MC service list (see NOTE)	O	List of MC services whose service communications are to be enabled on the group.
NOTE: This information element shall be included in the message for creating a group configured for multiple MC services.		

10.2.2.2 Group creation confirmation response

Table 10.2.2.2-1 describes the information flow group creation confirmation response from the group management server to the group management client.

Table 10.2.2.2-1: Group creation confirmation response

Information element	Status	Description
MC service group ID	M	MC service group ID of the group

10.2.2.3 Group regroup request (group management client – group management server)

Table 10.2.2.3-1 describes the information flow group regroup request from the group management client to the group management server.

Table 10.2.2.3-1: Group regroup request

Information element	Status	Description
MC service group ID list	M	List of MC service group IDs to be combined
Security level (see NOTE)	O	Required security level for the temporary group
Priority level	O	Required priority level for the temporary group
NOTE: Security level refers to the configuration of media and floor control protection parameters as listed in Annex A.4, table A.4-1		

10.2.2.4 Group regroup response (group management server – group management client)

Table 10.2.2.4-1 describes the information flow group regroup response from the group management server to the group management client.

Table 10.2.2.4-1: Group regroup response

Information element	Status	Description
MC service group ID	O (NOTE)	MC service group ID of the temporary group
Result	M	Indicates the success or failure of group regroup
NOTE: Shall be present if the Result information element indicates that the group regroup operation is successful. Otherwise MC service group ID shall not be present.		

10.2.2.5 Group regroup teardown request

Table 10.2.2.5-1 describes the information flow group regroup teardown request from the group management client to the group management server.

Table 10.2.2.5-1: Group regroup teardown request

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

10.2.2.6 Group regroup teardown response

Table 10.2.2.6-1 describes the information flow group regroup teardown response from the group management server to the group management client.

Table 10.2.2.6-1: Group regroup teardown response

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

10.2.2.7 Group creation notify

Table 10.2.2.7-1 describes the information flow group creation notify from the group management server to the MC service server(s).

NOTE: When group is configured for multiple MC services, the group creation notify message is sent from the group management server to the MC service servers configured for the group.

Table 10.2.2.7-1: Group creation notify

Information element	Status	Description
MC service group ID	M	MC service group ID that was created based on the MC service ID list and the MC services enabled on them
MC service ID list	M	List of MC service IDs that are part of the created group

10.2.2.8 Group regroup notify

Table 10.2.2.8-1 describes the information flow group regroup notify from the group management server to the MC service server.

Table 10.2.2.8-1: Group regroup notify

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

10.2.2.9 Group regroup teardown notify

Table 10.2.2.9-1 describes the information flow group regroup teardown notify from the group management server to the MC service server.

Table 10.2.2.9-1: Group regroup teardown notify

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

10.2.2.10 Group regroup teardown notification

Table 10.2.2.10-1 describes the information flow group regroup teardown notification between group management servers.

Table 10.2.2.10-1: Group regroup teardown notification

Information element	Status	Description
MC service group ID	M	MC service group ID of the temporary group which is torn down

10.2.2.11 Group regroup teardown notification response

Table 10.2.2.11-1 describes the information flow group regroup teardown notification response between group management servers.

Table 10.2.2.11-1: Group regroup teardown notification response

Information element	Status	Description
MC service group ID	M	MC service group ID of the temporary group which was torn down
Result	M	Indicates the success or failure

10.2.2.12 Group regroup request (group management server – group management server)

Table 10.2.2.12-1 describes the information flow group regroup request between group management servers.

Table 10.2.2.12-1: Group regroup request

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

10.2.2.13 Group regroup response (group management server – group management server)

Table 10.2.2.13-1 describes the information flow group regroup response between group management servers.

Table 10.2.2.13-1: 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
MC service group ID list	M	List of constituent MC service group IDs from group management server of the partner system

10.2.2.14 Group regroup notification

Table 10.2.2.14-1 describes the information flow group regroup notification between group management servers.

Table 10.2.2.14-1: Group regroup notification

Information element	Status	Description
MC service group ID list	M	List of constituent MC service group IDs
MC service group ID	M	MC service group ID of the temporary group
Priority level	O	Required priority level for the temporary group
Security level (see NOTE)	O	Required security level for the temporary group
NOTE: Security level refers to the configuration of media and floor control protection parameters as listed in Annex A.4, table A.4-1		

10.2.2.15 Group regroup notification response

Table 10.2.2.15-1 describes the information flow group regroup notification response between group management servers.

Table 10.2.2.15-1: Group regroup notification response

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

10.2.2.16 Group information query request

Table 10.2.2.16-1 describes the information group information query request from group management client to group management server.

Table 10.2.2.16-1: Group information query request

Information element	Status	Description
MC service ID	M	The identity of the MC service user who performs the query.
MC service group ID	M	The identity of the MC service group to be queried.
Query type	M	It indicates the query type, i.e., membership or affiliated group members.

10.2.2.17 Group information query response

Table 10.2.2.17-1 describes the information group information query response from group management server to group management client.

Table 10.2.2.17-1: Group information query response

Information element	Status	Description
MC service ID	M	The identity of the MC service user who performs the query.
MC service group ID	M	The identity of the MC service group to be queried.
Query type	M	It indicates the query type, e.g., membership or affiliated group members.
Query result	M	The group information retrieved from the group management server based on the query type, i.e., a list of group members or a list of affiliated group member.

10.2.2.18 Group membership update request

Table 10.2.2.18-1 describes the information flow group membership update request from the group management client to the group management server.

Table 10.2.2.18-1: Group membership update request

Information element	Status	Description
MC service group ID	M	Identity of the MC service group
MC service ID list	M	List of identities of the MC service users that are affected by this operation
Operations	M	Add to or delete from the group

10.2.2.19 Group membership update response

Table 10.2.2.19-1 describes the information flow group membership update response from the group management server to the group management client.

Table 10.2.2.19-1: Group membership update response

Information element	Status	Description
MC service group ID	M	Identity of the MC service group
Result	M	Indicates the success or failure for the operation

10.2.2.20 Group membership notification

Table 10.2.2.20-1 describes the information flow group membership notification from the group management server to the MC service server.

Table 10.2.2.20-1: Group membership notification

Information element	Status	Description
MC service group ID	M	Identity of the MC service group
MC service ID list	M	List of identities of the MC service users that are affected by this operation
Operations	M	Add to or delete from the group

Table 10.2.2.20-2 describes the information flow group membership notification from the group management server to the group management client.

Table 10.2.2.20-2: Group membership notification

Information element	Status	Description
MC service group ID	M	Identity of the MC service group
Operations	M	Add to or delete from the group

10.2.3 Group creation

Figure 10.2.3-1 below illustrates the group creation operations by authorized MC service user/ MC service administrator to create a group. It applies to the scenario of normal group creation by an MC service administrator and user regrouping operations by authorized user/dispatcher.

Pre-conditions:

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

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

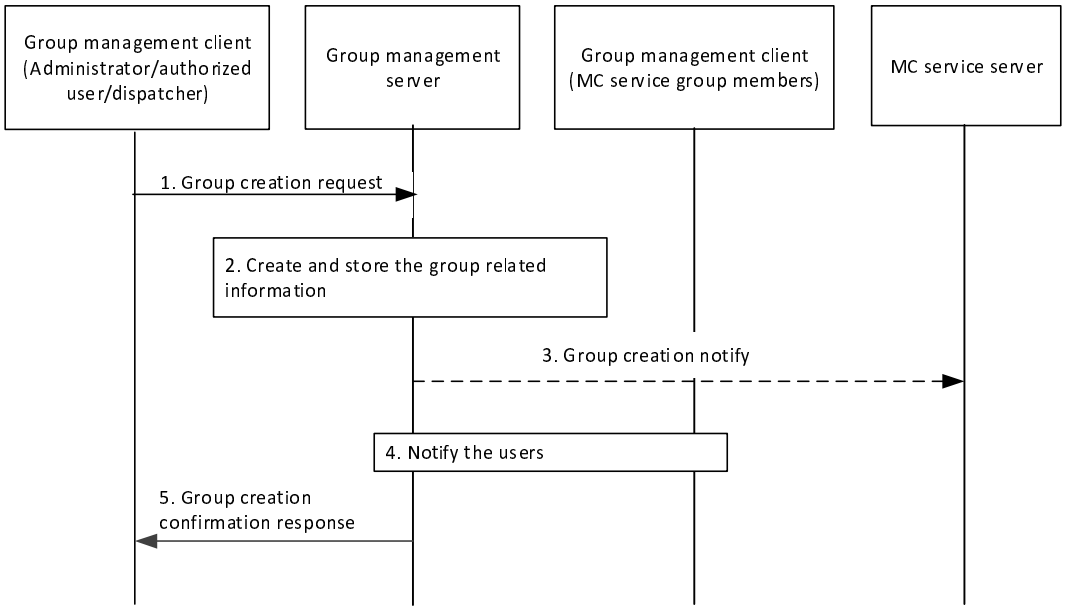

Figure 10.2.3-1: Group creation

1. The group management client of the administrator/dispatcher/authorized MC service user requests group create operation to the group management server. The identities of the users being combined and the information of the MC services that are enabled on the group 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 (Nc6) of MC service group members for the MC service group(s).

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

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

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

10.2.4 Group regrouping

10.2.4.1 Temporary group formation - group regrouping within an MC system

Figure 10.2.4.1-1 below illustrates the group regroup operations to create a temporary group within an MC system. For simplicity, only the case of two MC service groups being combined is represented, but the procedure is the same if more than two groups are combined.

NOTE: The temporary group formation is applicable only for groups configured with the same MC service(s).

Pre-conditions:

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

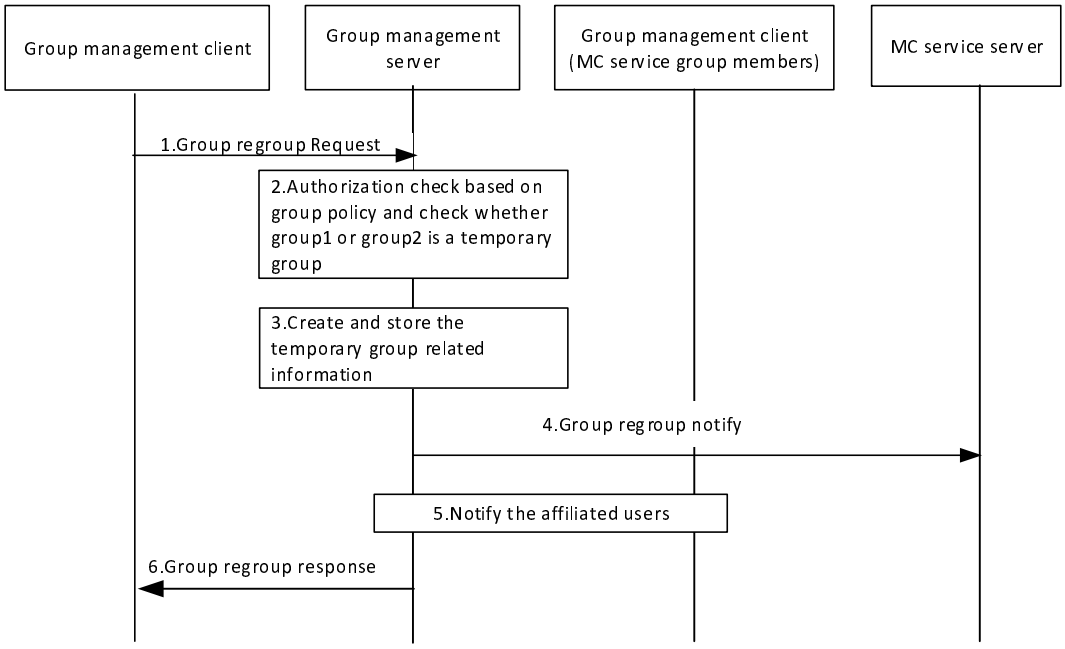

Figure 10.2.4.1-1: Group regroup for the groups within the same MC system

1. The group management client of the MC service user requests group regroup operation to the group management server, where the groups being combined are within the same MC 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 group regroup operation is performed by an authorized MC service user, based on group policy. 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 MC service group ID, the MC service group ID of the groups being combined, the priority level of the temporary group and the security level of the temporary group. If the authorized MC service 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 MC service server regarding the temporary group creation with the information of the constituent groups, i.e. temporary MC service group ID, group1's MC service group ID and group2's MC service group ID.

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

6. The group management server provides a group regroup response to the group management client of the authorized MC service user.

Editor's note: The temporary group formation for different MC services belonging to the same mission critical system is FFS.

10.2.4.2 Temporary group formation involving multiple MC systems

Figure 10.2.4.2-1 below illustrates the group regroup operations to create a temporary group involving multiple MC systems. For simplicity, only the case of two MC service groups being combined is represented, but the procedure is the same if more than two groups are combined.

NOTE: The temporary group formation is applicable only for groups configured with the same MC service(s).

Pre-conditions:

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

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

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

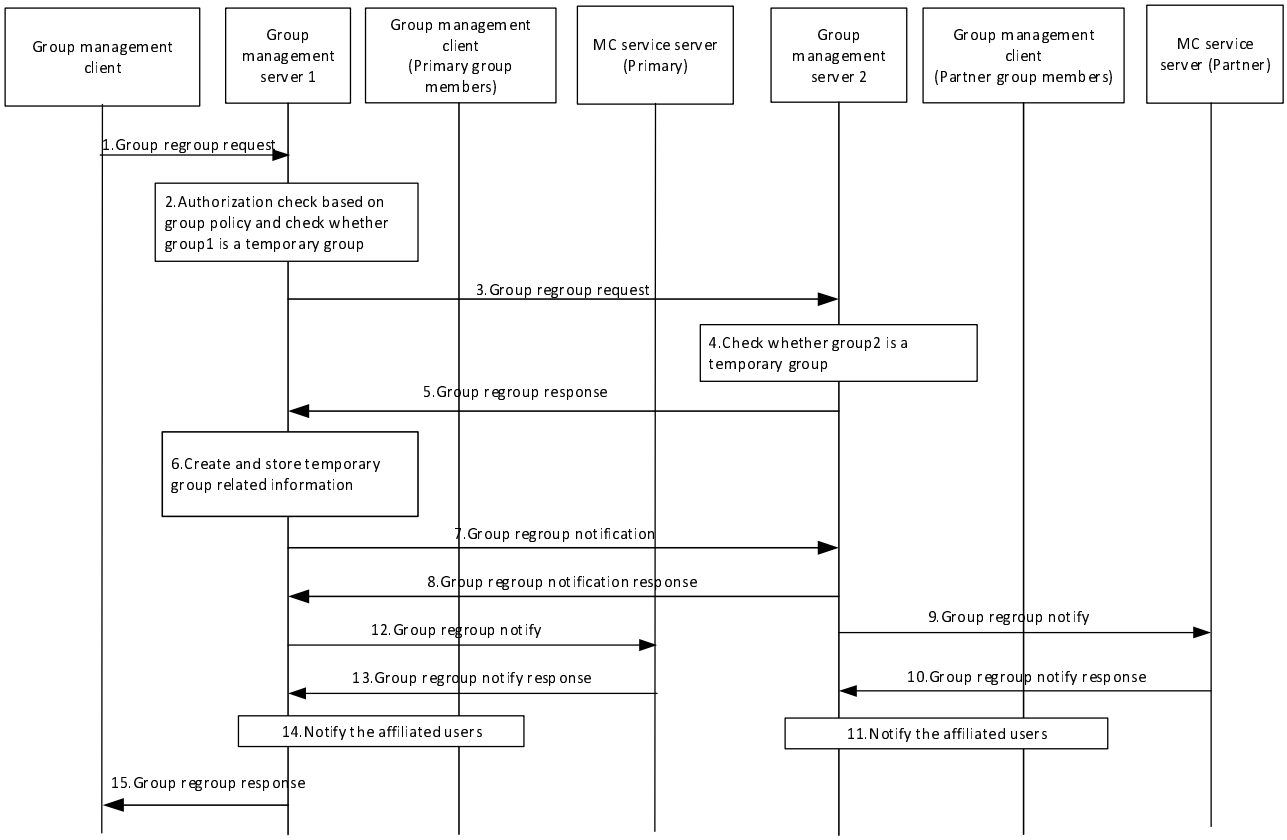

Figure 10.2.4.2-1: Temporary group formation - group regrouping involving multiple MC systems

1. The group management client of the MC service user (e.g. dispatcher) requests group regroup operation to the group management server 1 (which is the group management server of the authorized MC service 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 checks whether group regroup operation is performed by an authorized MC service user, based on group policy. 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 MC service 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 MC 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 MC service provider and the partner MC service provider, the partner MC system can share their users' information to the primary MC system at this step. If there is a change in partner MC system’s constituent group membership, the synchronization procedure with the primary MC 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 MC service group ID, off-network information, and the MC service IDs of the groups being combined, the priority level of the temporary group, and the security level of the temporary group. If the authorized MC service 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 MC service group ID, the MC service group IDs 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 MC service server regarding the temporary group creation with the information of the constituent groups i.e. temporary MC service group ID, group1's MC service group ID and group2's MC service group ID.

10. Partner MC service server acknowledges the notification from the group management server 2.

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

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

13. Primary MC service server acknowledges the notification from the group management server 1.

14. The group management server 1 notifies the affiliated MC service group members of the constituent MC service 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 response to the group management client of the authorized MC service user (e.g. dispatcher).

Editor's note: The temporary group formation for different MC services belonging to multiple mission critical system is FFS.

10.2.4.3 Temporary group tear down involving multiple group host servers

Figure 10.2.4.3-1 below illustrates the tearing down procedure of temporary group created through the group regroup operation. 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 MC service 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 MC systems shall be governed as per the service provider agreement between them. In this case, it considers the partner MC system does not share their users' information to the primary MC system.

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

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

4. The temporary group to be torn down is comprised of multiple MC service groups, and is created through the group regrouping procedure as described in subclause 10.2.4.2.

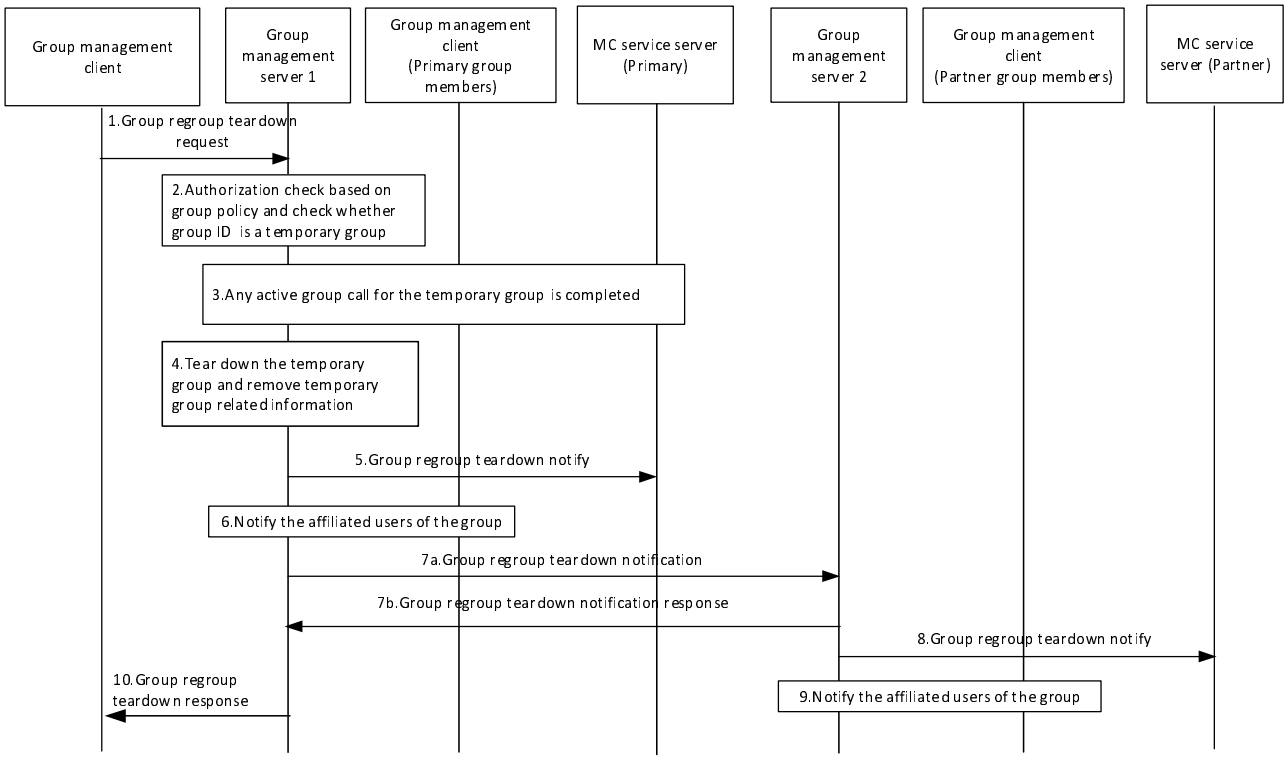

Figure 10.2.4.3-1: Temporary group tear down

1. The group management client of the MC service 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 (MC service 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 checks whether group regroup operation is performed by an authorized MC service user, based on group policy. The group management server 1 checks whether the MC service group ID is a temporary group. If MC service 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 MC service server regarding the temporary group teardown.

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

7. The group management server 1 sends a group regroup teardown notification (7a) and receives a group regroup teardown notification response (7b) messages with the group management server 2 – group management server in another MC system regarding the temporary group teardown.

8-9. The group management server 2 notifies the partner MC service server and the affiliated MC service 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 MC systems.

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

10.2.5 Membership and affiliation list query

10.2.5.1 General

An MC service user can request the membership or affiliation list on an MC service group regardless the user's group membership or affiliation.

10.2.5.2 Procedure

Figure 10.2.5.2-1 below illustrates the membership or affiliation list query on an MC service group.

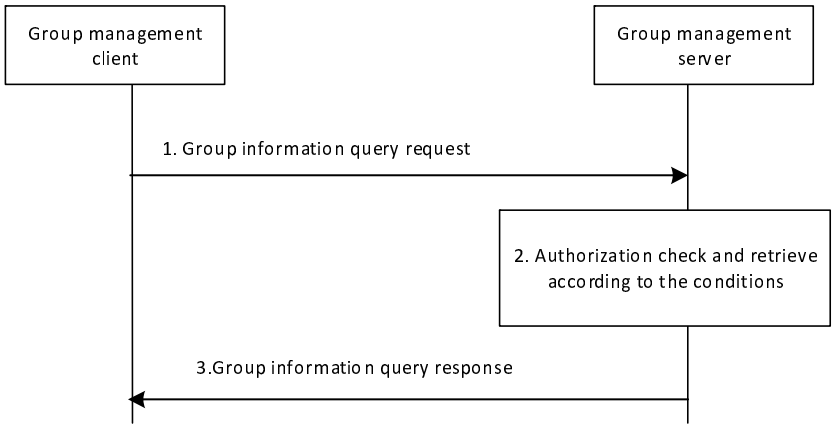

Figure 10.2.5.2-1: membership or affiliation list query

1. The group management client of the MC servicer user requests the membership or affiliation list on the MC service group from the group management server by sending a group information query request. The query type is included.
2. The group management server checks whether the MC servicer user is authorized to perform the query. If authorized, then the group management server retrieve the requested group information based on the query type.
3. The group management server sends a group information query response including the retrieved group information to the group management client.

10.2.6 Group membership

10.2.6.1 Group membership notification

Figure 10.2.6.1-1 illustrates the group membership notification operations to the MC service server(s) and group management clients upon the group membership change at group management server.

Pre-conditions:

1. The group management server and MC service server serve the same MC system.

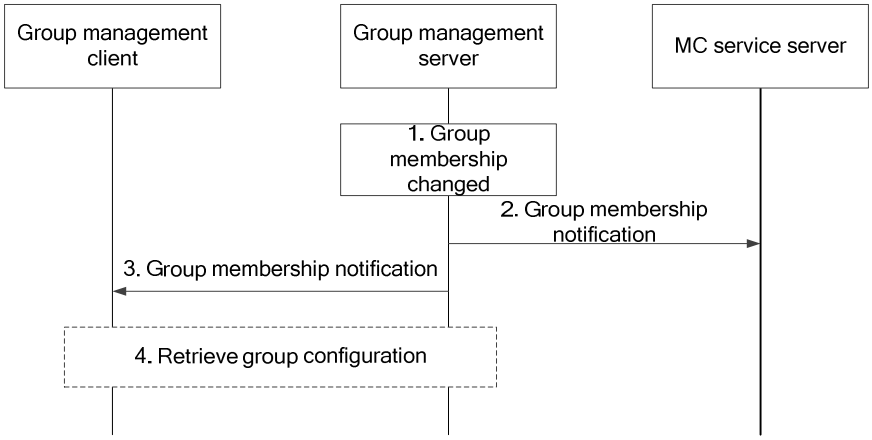

Figure 10.2.6.1-1: group membership notification

1. The membership of a specific MC service group is changed at group management server.
2. The group management server notifies the MC service server(s) regarding the group membership change with the information of the updated group members.
3. The group management server updates the group management clients of the MC service users who have been added to or removed from the group.
4. The group management client requests to retrieve the relevant group configurations from group management server by procedure defined in subclause 10.1.5.2, if the user is added to the group. If the user is deleted from the group, the locally stored group configurations in the MC service UE may be removed.

10.2.6.2 Group membership update by authorized user

Figure 10.2.6.2-1 below illustrates the group membership update operations by an authorized user/administrator/dispatcher to change the membership a MC service group (e.g. to add or delete group members).

Pre-conditions:

1. The group management server and MC service server serve the same MC service system;
2. The initiator of this operation is aware of the current group membership of the MC service group;
3. The Administrator/dispatcher/authorized user is aware of the users' identities which will be added to or deleted from the MC service group.

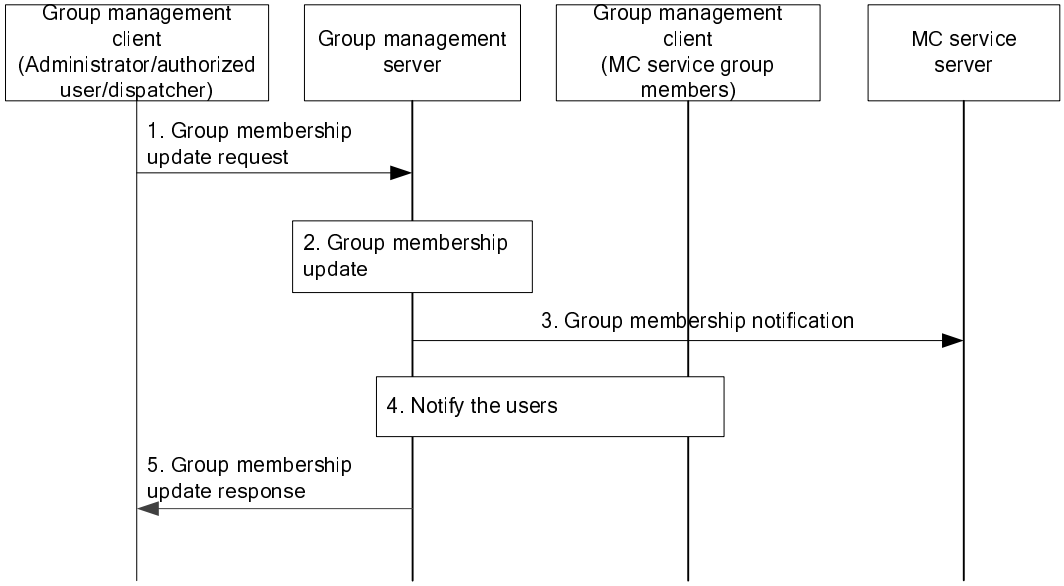

Figure 10.2.6.2-1: Group membership update by authorized user

1. The group management client of the administrator/dispatcher/authorized user requests group membership update operation to the group management server.
2. The group management server updates the group membership information. The group management server may perform the check on the maximum limit of the total number (Nc6) of MC service group members.
3. The group management server notifies the MC service server(s) regarding the group membership change with the information of the updated group members.
4. The group members that are added to or deleted from the group by this operation are notified about the group membership change. This step may be followed by retrieving group configurations defined in subclause 10.1.5.2
5. The group management server provides a group membership response to the group management client of the administrator/dispatcher/authorized user.

10.3 Pre-established session (on-network)

10.3.1 General

A pre-established session is a session established between an MC service client and the MC service server, on a per MC service basis, to exchange necessary media parameters needed for the definition of media bearers, allowing a faster set-up of MC service calls/sessions.

After a pre-established session is established, a media bearer carrying the media and media control messages is always active. The MC service client establishes one or more pre-established sessions to an MC service server after SIP registration, and prior to initiating any MC service related procedures (e.g. calls, sessions) to other MC service users. When establishing a pre-established session, the MC service client negotiates the media parameters, including establishing IP addresses and ports using interactive connectivity establishment (ICE) as specified in IETF RFC 5245 [22], which later can be used in MC service calls/sessions. This avoids the need to negotiate media parameters (including evaluating ICE candidates) and reserving bearer resources during the MC service call/session establishment that results in delayed MC service call/session establishment.

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 MC service client and the MC service server using the SIP procedures for session modification.

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

10.3.2 Procedures

10.3.2.1 General

The pre-established session can be established after MC service authorization for the user (see 3GPP TS 23.379 [16]).

The pre-established session is a session establishment procedure between the MC service client and the MC service 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 MC service 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 MC service call is initiated.

10.3.2.2 Pre-established session establishment

The pre-established session is a session between the MC service client and the MC service server in the MC 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 10.3.2.2-1 represents the pre-established session establishment flow.

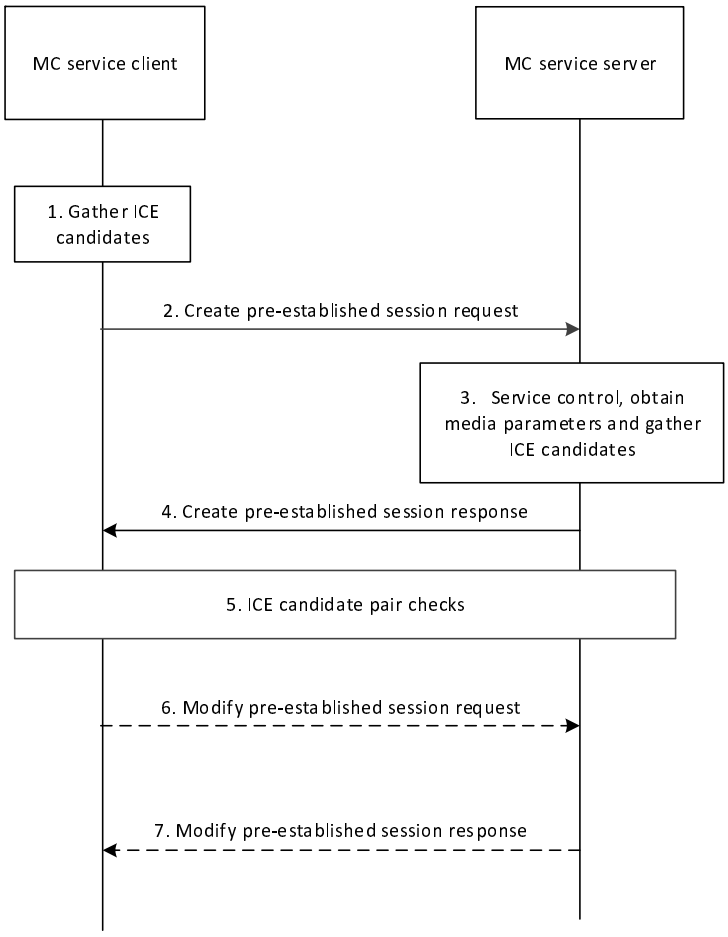

Figure 10.3.2.2-1: Pre-established session establishment

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

The media sessions consist of at least an active media session carrying the media and media control messages and an inactive media session for the media.

10.3.2.3 Pre-established session modification

Figure 10.3.2.3-1 represents the pre-established session modification flow.

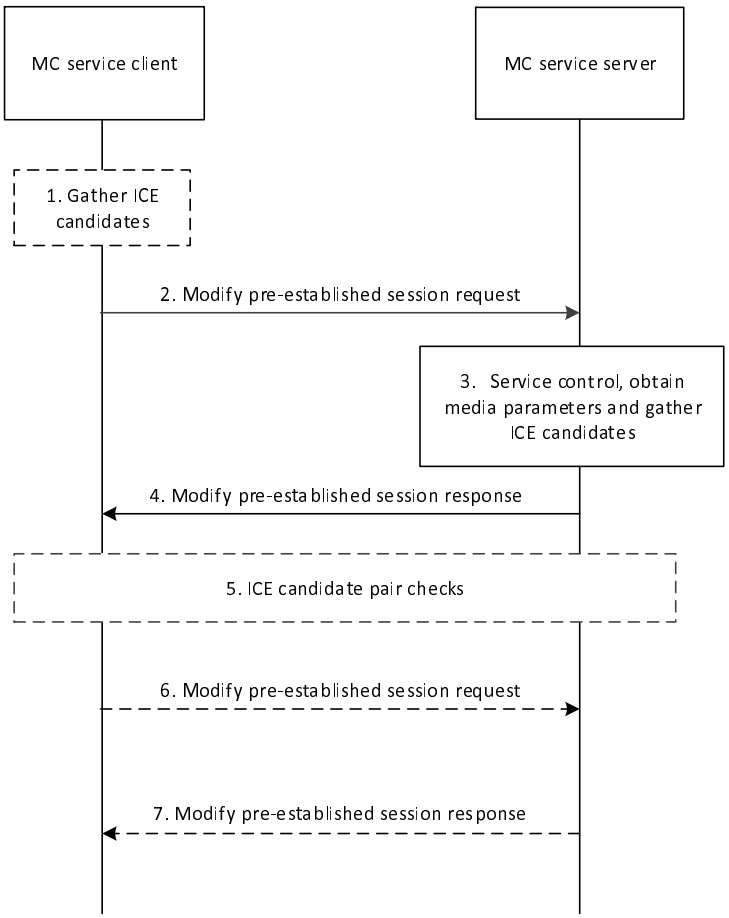

Figure 10.3.2.3-1: Pre-established session modification

1. The MC service client within the MC service UE gathers ICE candidates, if necessary (e.g. depending on the information that needs to be updated).
2. The MC service client within the MC service UE sends a request to the MC service server to modify a pre-established session.
3. MC service server performs necessary service control, obtains any necessary media parameters (e.g. by means of interacting with a media distribution function of the MC service server) and gathers necessary ICE candidates.
4. MC service server sends a modify pre-establish session response to the MC service client within the MC service UE.
5. If necessary, ICE candidate pair checks take place e.g. between the MC service client within the MC service UE and a media distribution function of the MC service server.
6. If necessary the MC service client within the MC service UE sends a modify pre-established session request to the MC service server to update the ICE candidate pair for the pre-established session.
7. The MC service server sends a modify pre-established session response accepting the ICE candidate pair update.

NOTE 1: The represented procedure corresponds to a session modification initiated by the MC service client. It can also be initiated by the MC service 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 (e.g. activity, bandwidth) of the corresponding GBR bearers.

10.3.2.4 Pre-established session release

Figure 10.3.2.4-1 represents the MC service client within the MC service UE initiated pre-established session release flow and figure 10.3.2.4-2 represents the MC service server initiated pre-established session release flow.

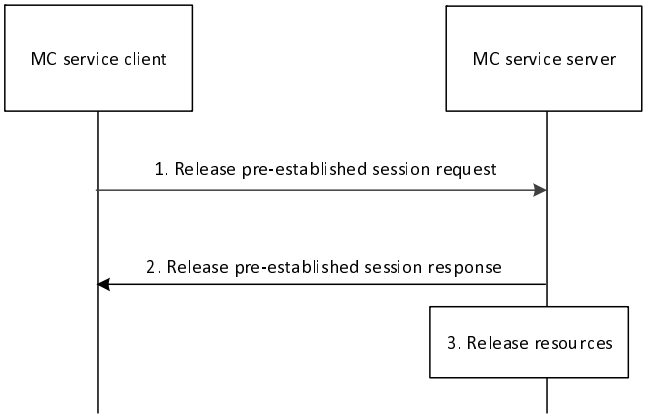

Figure 10.3.2.4-1: MC service client within the MC service UE initiated pre-established session release

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

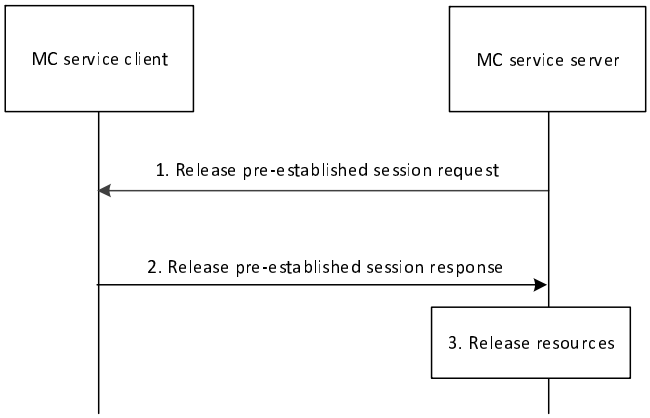

Figure 10.3.2.4-2: MC service server initiated pre-established session release

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

10.4 Simultaneous session (on-network)

10.4.1 General

A simultaneous session is functionality whereby the MC service client can receive the media from multiple MC service calls/sessions over the same SIP session and media bearer(s) between the MC service client and the MC service server.

10.5 Use of UE-to-network relay

10.5.1 UE-to-network relay service authorization

The MC 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 [14]) can be used with an appropriate relay service code as per the following:

- To restrict connection from only the membership of allowed MC service groups, UE-to-network relay UE is provisioned with relay service code(s) associated with allowed MC service group(s). The UE-to-network relay performs the access control as follows:

  1) The UE broadcasts which MC service 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 [14]); 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 MC service group(s) which the MC service 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 MC service group(s) is/are carried in UE-to-Network Relay Discovery Announcement message (as specified in 3GPP TS 23.303 [14]; or

2) The remote UE includes the relay service code(s) associated with its MC service group(s) in Network Relay Discovery Solicitation message (as specified in 3GPP TS 23.303 [14]).

10.5.2 UE-to-network relay MC 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 MC service user on the remote UE requires to access the MC service via a ProSe UE-to-network relay.

The application layer signalling for the MC service user on a remote UE are identical to the application layer signalling for the MC service user on an on network UE.

10.6 General user authentication and authorization for MC services

NOTE: Figure 10.6-1 is a high level user authentication and authorization flow. 3GPP TS 33.179 [20] defines the specific user authentication and authorization architecture required by the MC services in order to realize the MC service user authentication and authorization requirements as defined in 3GPP TS 22.280 [3].

The user authentication process shown in figure 10.6-1 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 MC service server.

A procedure for user authentication is illustrated in figure 10.6-1. Other alternatives may be possible, such as authenticating the user within the SIP registration phase.

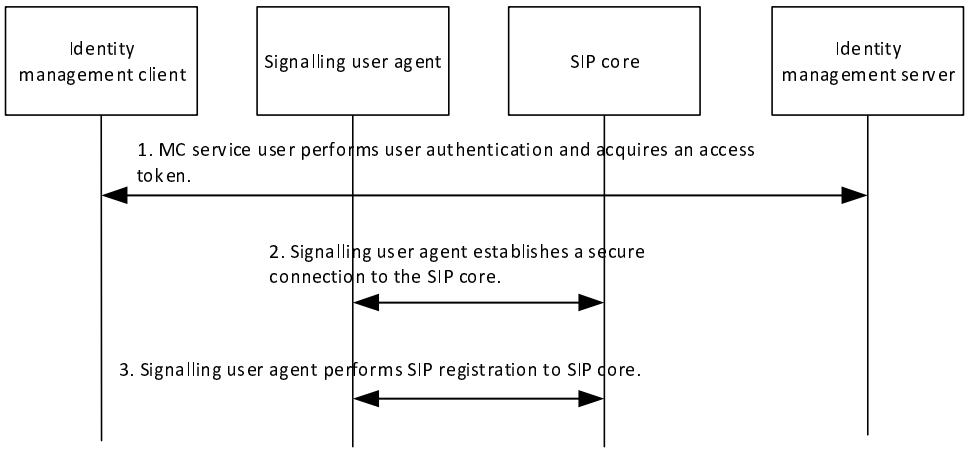

Figure 10.6-1: MC service user authentication and registration, single domain

1. In this step the identity management client begins the user authorization procedure. The MC service user supplies the user credentials (e.g. biometrics, secureID, username/password) for verification with the identity management server. This step may occur before or after step 3. In a MC system with multiple MC services, a single user authentication as in step 1 can be used for multiple MC service authorizations for the user.

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 MC service server(s)).

NOTE: The MC service client(s) perform the corresponding MC service authorization for the user by utilizing the result of this procedure.

10.7 Use of MBMS transmission

10.7.1 General

This subclause defines information flows and procedures for MBMS usage that applies to MC services. MBMS bearers can be used by any MC service for any MC service group. A single MBMS bearer can be used for one or more MC services within a single group or by multiple group communications in parallel.

The following subclauses specify the procedures and information flows for the usage of MBMS transmission that are utilised by the following MC services:

- MCPTT (as specified in 3GPP TS 23.379 [16]);
- MCVideo (as specified in 3GPP TS 23.281 [12]); and
- MCData (as specified in 3GPP TS 23.282 [13]).

MC service specific pre-requisites and resultant behaviour by functional entities in performing these procedures are specified in the respective MC service TSs as listed above.

10.7.2 Information flows for MBMS transmission

10.7.2.1 MBMS bearer announcement

Table 10.7.2.1-1 describes the information flow MBMS bearer announcement from the MC service server to the MC service client.

Table 10.7.2.1-1: MBMS bearer announcement

Information element	Status	Description
TMGI	M	TMGI information
Alternative TMGI	O	A list of additional alternative TMGI may be included and used in roaming scenarios.
QCI	O	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
List of service area identifier	M	A list of service area identifier for the applicable MBMS broadcast area.
Frequency	O	Identification of frequency if multi carrier support is provided
SDP information	M	SDP with media and floor control information applicable to groups that can use this bearer (e.g. codec, protocol id)
Monitoring state	O	The monitoring state is used to control if the client is actively monitoring the MBMS bearer or not.
Announcement acknowledgment	O	Indicate if the MBMS server requires an acknowledgement of the MBMS bearer announcement.
Unicast status	O	An indication that the listening status of the unicast bearer is requested.
NOTE: When MBMS bearer announcement is done on a MBMS bearer all attributes above are optional except the TMGI.		

10.7.2.2 MBMS listening status report

Table 10.7.2.2-1 describes the information flow for the MBMS listening status report from MC service client to MC service server. The information is used for the decision on the switching from MBMS bearer to unicast bearer or vice versa.

Table 10.7.2.2-1: MBMS listening status report

Information element	Status	Description
MC service ID	M	The identity of the MC service user who wants to report the MBMS listening status.
TMGI(s)	M	TMGI(s) information.
MBMS listening status(s)	M	The MBMS listening status per TMGI.
Unicast listening status	O	The unicast listening status.

10.7.2.3 MBMS suspension reporting instruction

Table 10.7.2.3-1 describes the information flow for the MBMS suspension reporting instruction from MC service server to MC service client in a unicast bearer for MBMS suspension reporting.

Table 10.7.2.3-1: MBMS suspension reporting instruction (unicast)

Information element	Status	Description
MC service ID	M	The MC service identity
Suspension reporting	M	Enables or disable the suspension reporting for a specific MC service client

Table 10.7.2.3-2 describes the information flow for the MBMS suspension reporting instruction from MC service server to MC service client in a multicast bearer for MBMS suspension reporting.

Table 10.7.2.3-2: MBMS suspension reporting instruction (multicast)

Information element	Status	Description
Suspension reporting client subset	M	Contains a uniquely defined subset of MC service clients that shall report MBMS suspension

10.7.2.4 Discover bearer request

Table 10.7.2.4-1 describes the information flow discover bearer request from the MC service server (controlling role) to another MC service server (participating and/or MBMS bearer owning role).

Table 10.7.2.4-1: Discover bearer request

Information element	Status	Description
List of service area identifiers	M	A list of service area identifier for the applicable MBMS broadcast area.
Bandwidth	M	Maximum bandwidth required
QCI	O	Desired QCI

10.7.2.5 Discover bearer response

Table 10.7.2.5-1 describes the information flow discover bearer response from an MC service server (participating and/or MBMS bearer owning role) to the MC service server (controlling role).

Table 10.7.2.5-1: Discover bearer response

Information element	Status	Description
TMGIs	M	List of TMGIs and related information
List of service area identifiers	M	A list of service area identifiers for the applicable MBMS broadcast areas, corresponding to the listed TMGIs, over which the request was successful.
Frequency	O	Identification of the frequency if multi-carrier support is provided
QCI	O	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 a remote UE over PC5.

10.7.2.6 Media distribution request

Table 10.7.2.6-1 describes the information flow media distribution request from the MC service server (controlling role) to an MC service server (participating and/or MBMS bearer owning role) that has a desired bearer.

Table 10.7.2.6-1: Media distribution request

Information element	Status	Description
TMGI	M	TMGI information
Bandwidth	M	Maximum bandwidth required
Separate floor control	M	Whether or not a separate bearer is required for floor control
SDP information	M	SDP with media and floor control information applicable to groups that can use this bearer (e.g. codec, protocol id)
QCI	O	Desired QCI

10.7.2.7 Media distribution response

Table 10.7.2.7-1 describes the information flow media distribution response from an MC service server (participating and/or MBMS bearer owning role) that has a desired bearer to the MC service server (controlling role).

Table 10.7.2.7-1: Media distribution response

Information element	Status	Description
TMGI	M	TMGI information
Bandwidth	M	Maximum bandwidth required
SDP information	M	SDP with media and floor control information applicable to groups that can use this bearer (e.g. codec, protocol id)
QCI	O	Actual QCI

10.7.2.8 Identify multicast participants request

Table 10.7.2.8-1 describes the information flow identify multicast participants request from the MC service server (controlling role) to an MC service server (participating role).

Table 10.7.2.8-1: Identify multicast participants request

Information element	Status	Description
MC group ID	M	The MC service group ID of the group on which the call is requested
MC user ID list	M	The list of MC service IDs of the MC service group members who are expected to be receiving multi-cast

10.7.2.9 Remove call from bearer request

Table 10.7.2.9-1 describes the information flow remove call from bearer request from the MC service server (controlling role) to an MC service server (MBMS bearer controlling role).

Table 10.7.2.9-1: Remove call from bearer request

Information element	Status	Description
TMGI	M	TMGI information
MC group ID	M	The MC service group ID of the group on which the call is requested

10.7.3 Procedures for MBMS usage

Editor's note: The procedures defined in this subclause are utilized by each MC service servers individually. It is FFS if the use of MBMS bearer(s) can be managed by a centralized MBMS management server.

10.7.3.1 Use of pre-established MBMS bearers

10.7.3.1.1 General

In this scenario, the MC service server pre-establishes MBMS bearer(s) in certain pre-configured areas before the initiation of the group communication session. When a user originates a request for a group communication session 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 MC group communication session over pre-established MBMS bearer:

- MBMS bearer(s) is Pre-established
- Announce the pre-established MBMS bearer to the MC service clients

When these preparation steps have been done the MC group communication session using MBMS bearer can start.

Both the media packets as well as the application level control signalling (e.g. floor control messages) to the receiving MC service clients are sent on the MBMS bearer. Optionally a separate MBMS bearer could be used for the application level control messages, due to different bearer characteristic requirements.

10.7.3.1.2 Procedure

The procedure figure 10.7.3.1.2-1 shows only one of the receiving MC service clients using an MBMS bearer. There might also be MC service clients in the same MC group communication session that receive the communication on unicast bearers.

Pre-conditions:

- The participating users are already affiliated.

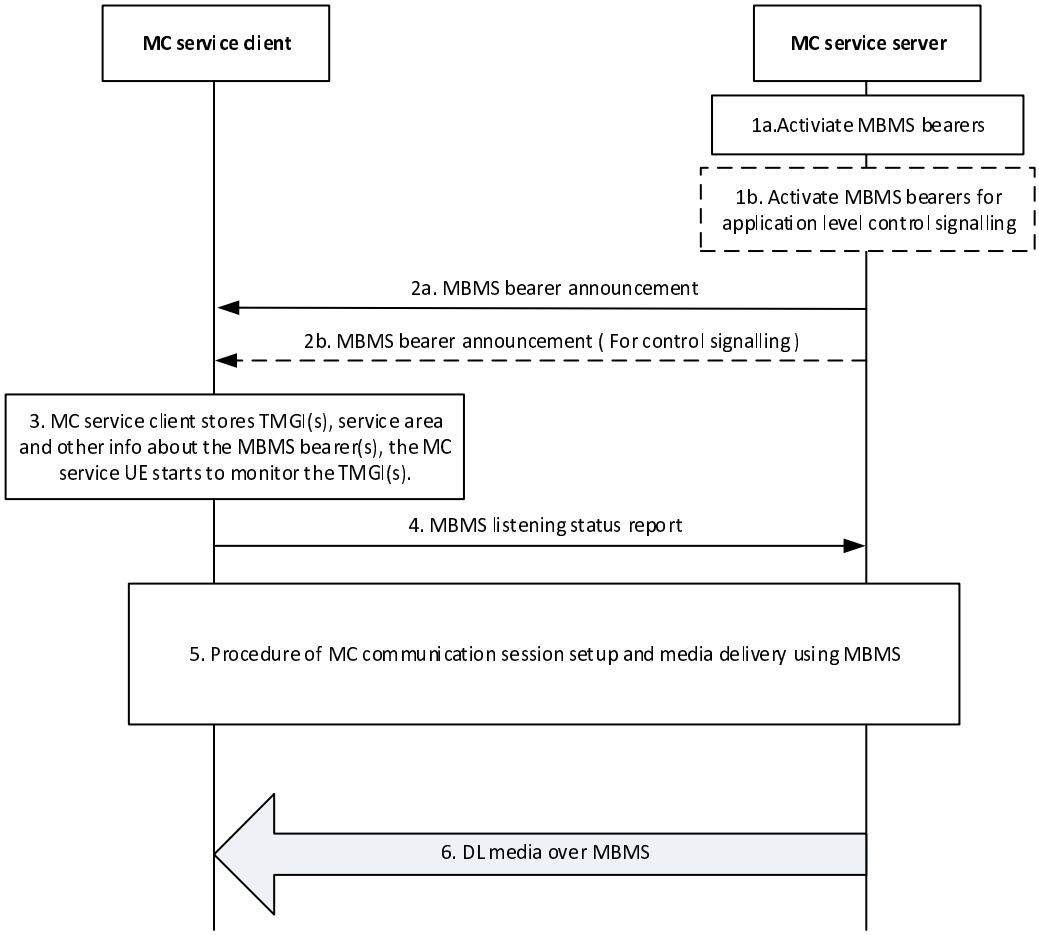

Figure 10.7.3.1.2-1: Use of pre-established MBMS bearers

1a. The MC service server determines to activate MBMS bearer. The activation of the MBMS bearer is done on the MB2-C reference point and according to 3GPP TS 23.468 [18]. This bearer will be used for the MC communication media.

1b. Optionally, the MC service server may also activate an MBMS bearer dedicated for application level control signalling. The activation of the MBMS bearer is done on MB2-C reference point and according to 3GPP TS 23.468 [18].

NOTE 1: The procedure to determine the activation of MBMS bearers is implementation specific.

2a. The MC service server passes the MBMS bearer info for the service description associated with the pre-established MBMS bearer to the MC service client. The MC service client obtains the TMGI, identifying the MBMS bearer, from the service description.

2b. The MC service server may pass the MBMS bearer info for the service description associated with the pre-established floor control MBMS bearer to the MC service client. The MC service 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 MC service client stores the information associated with the TMGI(s). The MC service client uses the TMGI and other MBMS bearer related information to activate the monitoring of the MBMS bearer by the MC service UE.

4. The MC service client that enters or is in the service area of at least one announced TMGI indicates to the MC service server that the MC service client is able to receive media over MBMS, whereby the MC service server may decide to use the MBMS bearer instead of unicast bearer for MC communication sessions.

NOTE 3: Step 4 is optional for the MC service UE on subsequent MBMS bearer announcements.

5. An MC service group communication session is established.

6. As the MC service server transmits the media over the MBMS bearer, the media packets are detected and delivered to the MC service client.

10.7.3.2 Use of dynamic MBMS bearer establishment

In this scenario depicted in figure 10.7.3.2-1, the MC service server uses a unicast bearer for communication with the UE on the DL at the start of the group communication session. When the MC service server decides to use an MBMS bearer for the DL media transmission, the MC service server establishes an MBMS bearer using the procedures defined in 3GPP TS 23.468 [18]. The MC service server provides MBMS service description information 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 MC service server logic for determining when to establish the new MBMS delivery bearer is implementation specific. For example, the MC service 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.

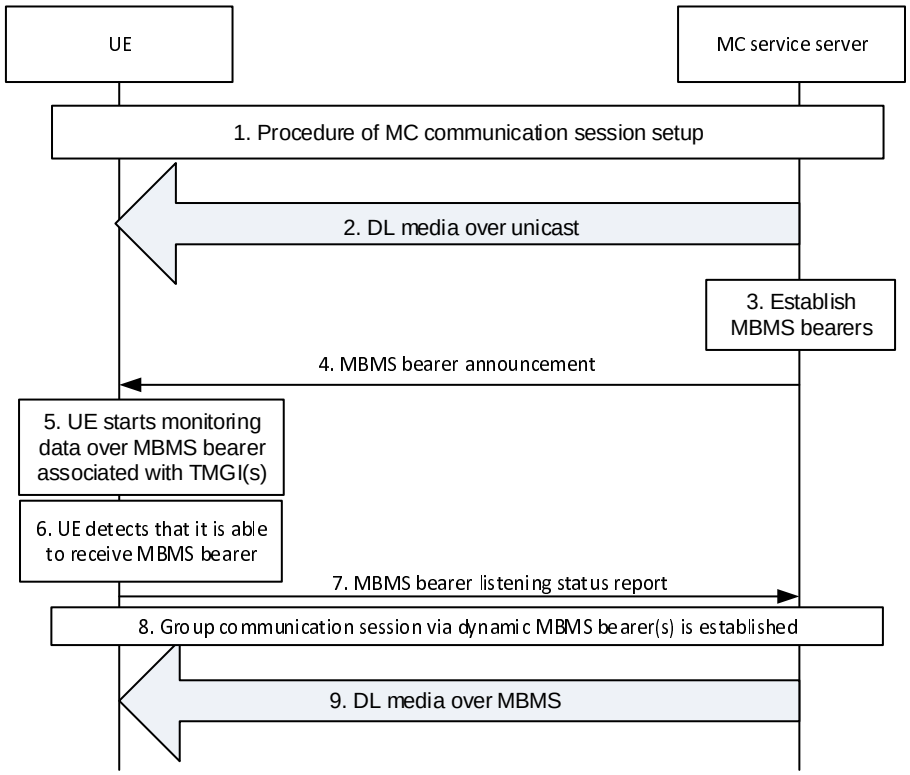

Figure 10.7.3.2-1: Use of dynamic MBMS bearer establishment

1. An MC service group communication session is established.

2. The downlink data is sent by unicast delivery.

3. The MC service server establishes the MBMS bearer(s) for the group communication session according to the procedures defined in 3GPP TS 23.468 [18]. Service description associated with the MBMS bearer(s) is returned from The BM-SC.

4. The MC service server provides service description information associated with the MBMS bearer to the UE. The MC service UE obtains the TMGI from the announcement message. This message may be sent on an application level control signalling bearer.

5. The MC service UE starts monitoring data over MBMS associated with the TMGI, while in the service area associated with the TMGI.

6. The MC service UE detects that it is able to receive data over MBMS associated with the TMGI.

7. The MC service client notifies the MC service server that it is successfully receiving the TMGI. MC service server stops sending media data over unicast way to the MC service client.

8. An MC service group communication session via dynamic MBMS bearer(s) is established.

NOTE 2: Step 8 can occur before step 7.

9. MC service server sends the downlink media for the group communication session over the MBMS.

10.7.3.3 Switching from MBMS bearer to unicast bearer

Figure 10.7.3.3-1 shows the procedure for service continuity when a UE is about to move out of MBMS coverage by switching from MBMS bearer to unicast bearer.

Pre-conditions:

- It is assumed that the MBMS bearer has been activated by MC service server for downlink delivery.

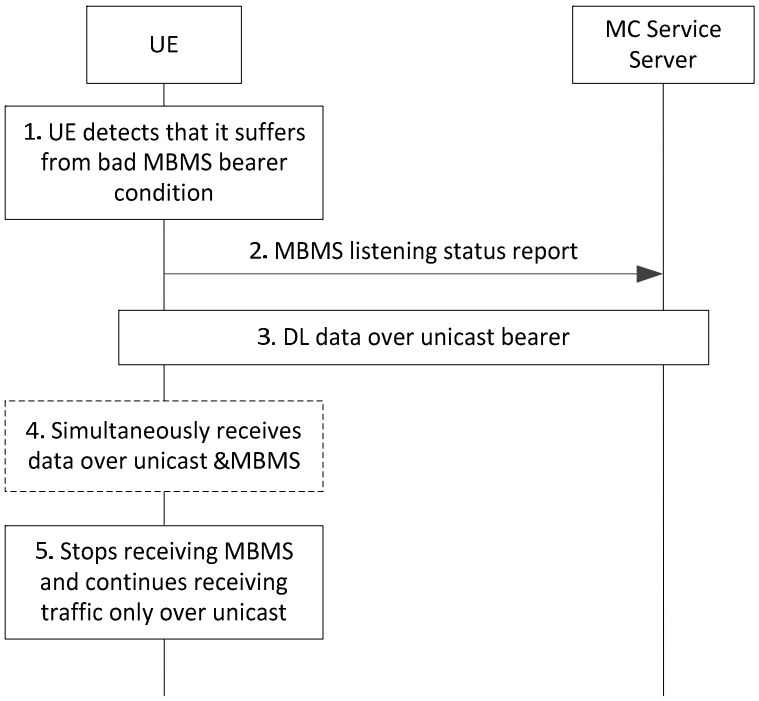

Figure 10.7.3.3-1: Switching from MBMS delivery to unicast delivery

1. The MC service UE detects that it suffers from bad MBMS bearer condition for the corresponding MBMS service. The method to detect is implementation specific.

2. The MC service client notifies the MC service server that it suffers from bad MBMS bearer condition for the corresponding MBMS service by sending the MBMS listening status report.

3. The MC service server sends the downlink data by unicast delivery to the MC service client.

NOTE: The unicast bearer may be set up on demand after step 2 or before.

4. During the switching, the MC service client simultaneously receives downlink data through both unicast bearer and MBMS bearer. If there is no downlink data to the MC service client, this step can be skipped.

5. The MC service client ceases to receive the downlink data through MBMS bearer but continues receiving data through unicast bearer.

10.7.3.4 Use of MBMS bearer for application level control signalling

10.7.3.4.1 Description

The MC service server may use an MBMS bearer for application level control signalling, according to this subclause. An MBMS bearer for application level control signalling is typically used for the purposes beyond the benefit for using MBMS for resource efficiency, e.g. for improved MC service performance (KPIs), handling of high load scenarios.

The MBMS bearer for application level control signalling may be used to transmit the following messages:

- Transmission control (e.g. call setup and floor control)
- MBMS bearer announcement for media bearers
- Group application paging
- Group configuration
- Group state (e.g. emergency alerts)

An MBMS bearer for application level control signalling is activated in a service area that is larger than the estimated service for media bearers. The service area for the media bearers mainly based on counting of group members in each defined service area. The MBMS bearer for application level control signalling is also activated with a QoS that is better than MBMS media bearers since the packet loss requirements are much stricter.

10.7.3.4.2 Procedure

The procedure in figure 10.7.3.4.2-1 shows only one of the receiving MC service clients using an MBMS bearer.

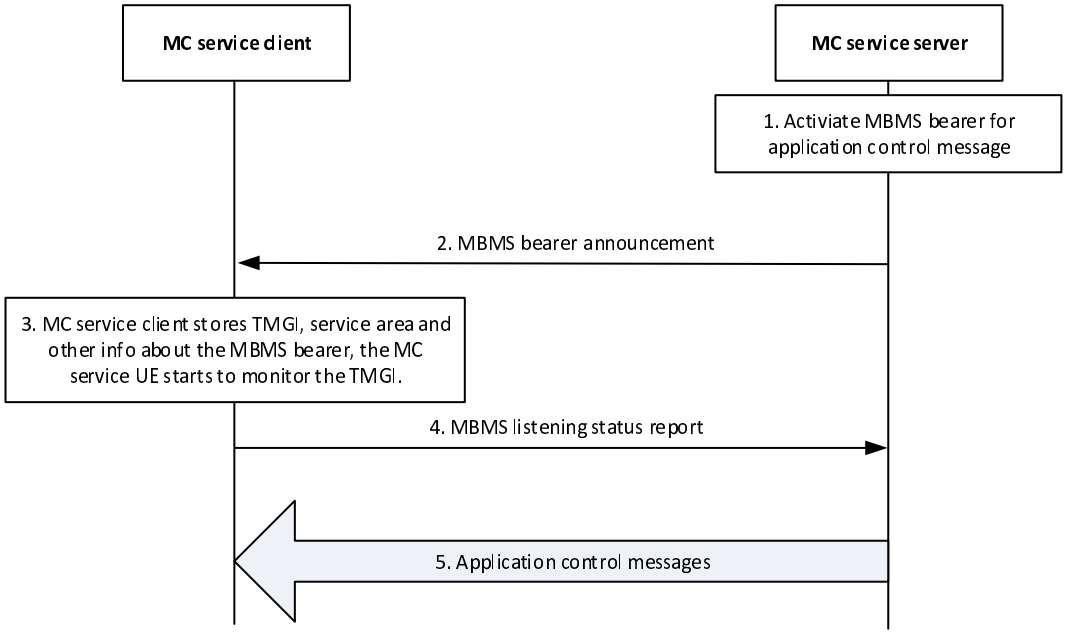

Figure 10.7.3.4.2-1: Use of MBMS bearer for application level control signalling

1. The MC service server determines to activate MBMS bearer for application level control signalling, The activation of the MBMS bearer is done on the MB2-C reference point and according to 3GPP TS 23.468 [18].
2. The MC service server passes the MBMS bearer info for the service description associated MBMS bearer to the MC service client. The MC service client obtains the TMGI, identifying the MBMS bearer, from the service description.
3. The MC service client stores the information associated with the TMGI. The MC service client uses the TMGI and other MBMS bearer related information to activate the monitoring of the MBMS bearer by the MC service UE.

4. The MC service client that enters or is in the service area of the announced TMGI indicates to the MC service server that the MC service client is able to receive application level control messages over the MBMS bearer, whereby the MC service server may decide to use the MBMS bearer for MC application control messages.

5. The MC service server transmit MC application control messages

10.7.3.5 MBMS bearer announcement over MBMS bearer

10.7.3.5.1 Description

The MBMS announcement may be done on either a unicast bearer or a MBMS bearer. Using a unicast bearer for MBMS bearer announcement provides an interactive way of doing announcement. The MC service server will send the MBMS bearer announcement message to the MC service client regardless if there is an MBMS bearer active or the MC service client can receive the data on the MBMS bearer with sufficient quality. The benefit of the existing procedure is that it gives a secure way to inform the MC service client about the MBMS bearer and how to retrieve the data on the MBMS bearer.

When there is more than one MBMS bearer active in the same service area for MC service, there are not the same reasons to use unicast bearer for additional MBMS bearer announcement. Instead a MBMS bearer for application level control signalling can be used to announce additional MBMS bearers.

The MBMS bearer announcement messages are sent on an MBMS bearer used for application control messages. This bearer will have a different QoS setting compared to an MBMS bearer used for media, since application signalling messages are more sensitive to packet loss.

10.7.3.5.2 Procedure

The procedure defined below enables the MC service to announcement a new MBMS bearer.

Pre-conditions:

- An MBMS bearer used for MC service application control messages must have been pre-established and announced to the MC service client.

- Additional MBMS bearer information may have already been announced to the client.

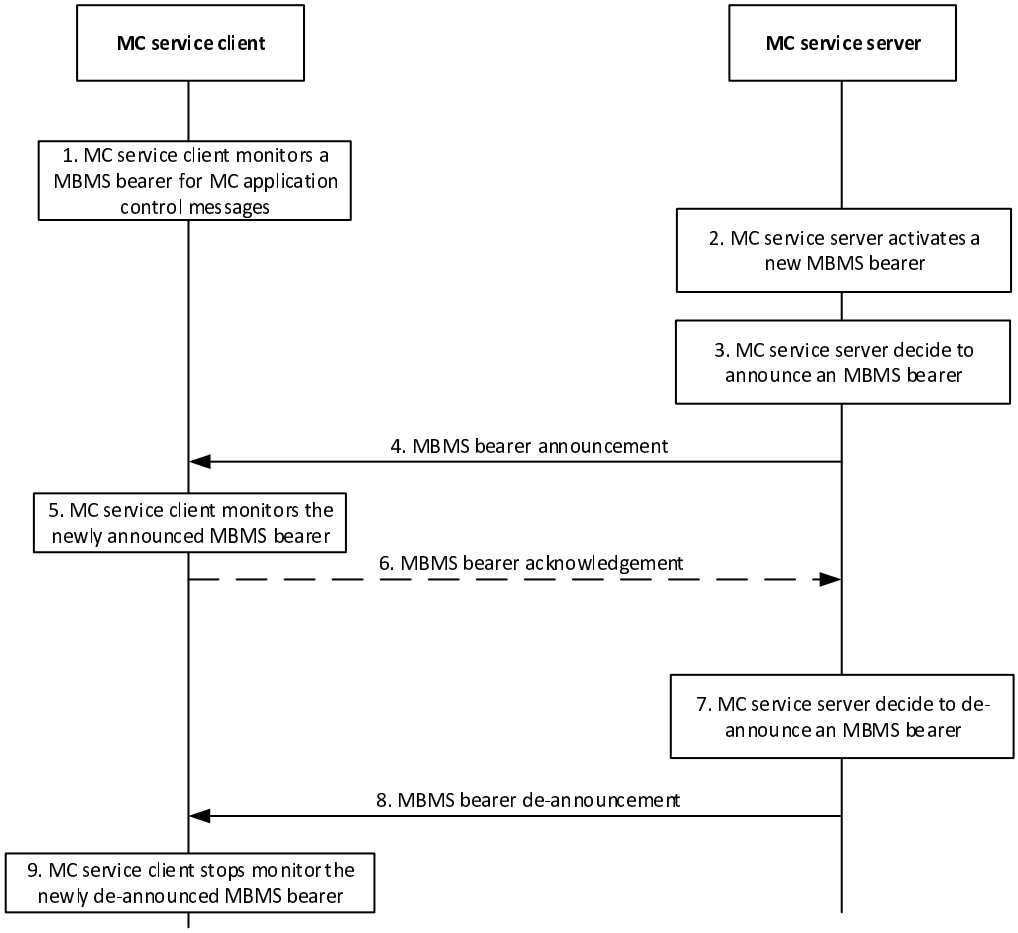

Figure 10.7.3.5.2-1: MBMS bearer announcement over an MBMS bearer used for application control messages

1. The MC service client monitors an MBMS bearer that is used for MC service application signalling messages, such as bearer announcement messages.

2. The MC service server activates a new MBMS bearer.

3. The MC service server announce the MBMS bearer to the MC service client. The bearer may have just been activated or may have already been running for some time. The step may be repeated as needed.

4. The MC service server sends a MBMS bearer announcement on the MBMS bearer used for MC application control messages. The MBMS bearer announcement contains the identity of the MBMS bearer (i.e. the TMGI) and may optionally include additional information about the newly announced bearer. Required and optional MBMS bearer announcement details may have already been provided. In this case the MBMS bearer identity could be used as a key for such MBMS bearer details.

5. The MC service clients start to monitor the newly announced MBMS bearer.

6. If requested by the MC service server, the MC service client sends an acknowledgement of the MBMS bearer to the MC service server.

7. The MC service server de-announce the MBMS bearer.

8. The MC service server sends a MBMS bearer de-announcement message that contains the identity of the MBMS bearer.

9. The MC service client stops monitoring the de-announced MBMS bearer.

The same procedure can also be used to modify existing MBMS bearer announcement information. Example of such modification could be addition of UDP ports or modification of codec in the SDP.

10.7.3.6 MBMS bearer quality detection

10.7.3.6.1 Description

The MC service client and MC service server use this procedure to report and take action on the MBMS bearer quality. An MC service client monitors an MBMS bearer to receive MC service media. Based on the received quality (e.g. radio level quality, transport level quality), the MC service client needs to inform the MC service server that the MC service client is able to receive the MC service media on the MBMS bearer with sufficient quality or not able to receive the MC service media on the MBMS bearer with sufficient quality.

The issue can be more complex since the MC service client needs to estimate the quality of the bearer even in the scenario when there are no data currently transmitted on the MBMS bearer (e.g. between MCPTT group call). The reason for this is that an MC service client that has entered an area with significantly degraded MBMS quality, might not even notice that an MC service communication is ongoing, meanwhile the MC server still assumes that the MC service client can receive the media being broadcasted.

To estimate the MBMS bearer quality, for example as an equivalent BLER (Block Error Rate) when no data is sent is implementation specific. This estimation is dependent on for example the modulation and coding scheme (MCS) and measurements from the reference signals from the eNB(s). Other metrics (e.g. RTP packet loss) may be used to estimate the MBMS bearer quality.

10.7.3.6.2 Procedure

The MC service client shall indicate the ability of the MC service client to receive the MBMS bearer.

Pre-conditions:

- There is an MBMS bearer activated and the MBMS bearer information is announced to the MC service client
- The MC service client is located in the MBMS broadcasting area
- The MC service UE monitors SIB-13 (or SIB-20) and (SC-)MCCH to receive the modulation and coding scheme
- The MC service UE monitors the cell specific reference signal and when MBSFN transmission is used, the MBSFN specific reference signals

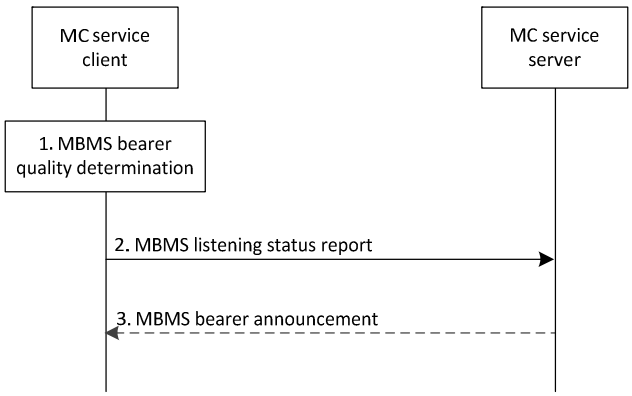

Figure 10.7.3.6.2-1: MBMS bearer quality detection

1. The MC service client determines that the MBMS bearer quality shall be reported to the MC service server. The MC service client may determine the MBMS bearer quality by using the BLER of the received data. When no data is received, the quality estimation should consider the reference signals and the modulation and coding scheme (MCS). The UE may also use predictive methods to estimate the expected MBMS bearer quality (e.g. speed and direction) to proactively inform the MBMS service server of an expected loss of the MBMS bearer quality.

NOTE 1: When MBSFN transmission is used, the MBSFN reference signal needs to be used and when SC-PTM is used the cell specific reference signal needs to be used. With the measured reference signal, the reference signal received quality (RSRQ) can be calculated.

2. If the MBMS bearer quality reaches a certain threshold, the MC service client sends an MBMS listening status report. The threshold used indicates that the MBMS bearer is not acceptable for MC services.

NOTE 2: Prior sending the MBMS listening status report, it could be beneficial to also include information for different alternatives e.g. another MBMS bearer might have better quality and could be a better option than a transfer of the communication to unicast.

NOTE 3: The threshold used to indicate MBMS bearer quality depends on service type (i.e. MCPTT, MCVideo or MCData) and the metrics used. The metrics used and the associated thresholds are out of scope of this specification.

3. The MC service server may send additional proposal for measurements e.g. information about neighbouring MBMS bearers. This message may be an MBMS bearer announcement message.

10.7.3.7 Service continuity in MBMS scenarios

10.7.3.7.1 General

This subclause specify service continuity scenario when MBMS bearers are used. There are different solutions for different scenarios.

10.7.3.7.2 Service continuity when moving from one MBSFN to another

The service continuity solution described in this subclause is suitable in the scenario when multiple MBMS bearers are used with the purpose to cover a larger area. In mission critical communication several media streams may be multiplexed in one MBMS bearer. Furthermore, one media stream (e.g. MCPTT group call) may be sent on more than one MBMS bearer if the receiving users are distributed over more than one MBMS service area. An MC service client that is interested in receiving a media stream that is broadcasted in both MBMS bearers is a candidate for this service continuity procedure.

Figure 10.7.3.7.2-1 illustrates a deployment scenario that provides service continuity between two MBSFN areas. Two different MBMS bearers are activated (TMGI 1 and TMGI 2), the activation of the bearers is done in the two MBSFN areas (MBSFN 1 and MBSFN 2). The MBSFN areas 1 and 2 are partially overlapping, meaning that some transmitting cells belong to both MBSFN area 1 and MBSFN area 2.

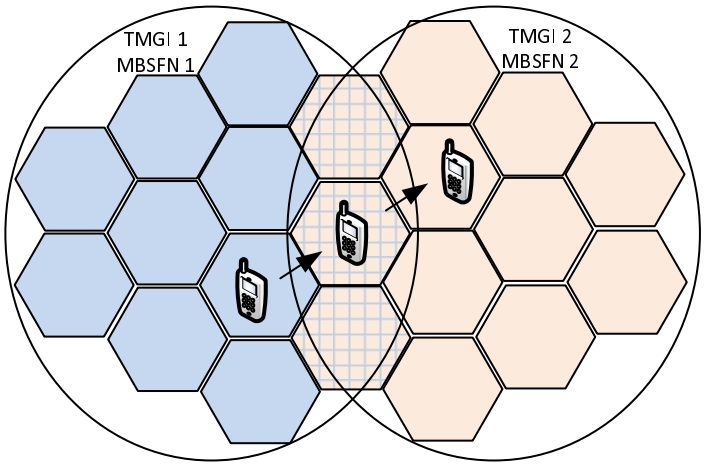

Figure 10.7.3.7.2-1: Two MBMS bearer using overlapping MBSFN areas

The procedural steps will work as follows:

1. The UE is located in MBSFN 1 and can listen to TMGI 1. No additional MBMS bearers that the MC service client is interested in are active in the current cell.

2. The UE moves into a new cell in which both TMGI 1 and TMGI 2 are active. This cell is part of both MBSFN area 1 and MBSFN area 2, and broadcast the same service on both TMGIs. After some seconds the UE detects the new MBMS bearer and detects that TMGI 2 broadcasts the same service. The UE may now listen to both TMGI 1 and TMGI 2 and receive duplicated packets. The MC service client must also verify that it is the same content sent on both bearers. The duplicated packets may also be used to perform error corrections.

NOTE: It is assumed that both MBMS bearers are announcement to the MC service client, and the MC service UE listen to SIB-13 and (SC-)MCCH to detect these MBMS bearers.

3. The UE moves into a new cell in which only TMGI 2 is active.

This service continuity procedure mitigates the risk of packet loss that may occur if the UE would request to transfer the media stream to a unicast bearer when moving into the new area and then back to a multicast bearer when the UE can listen to TMGI 2. However, it is still required that the MC service client sends a location report (and MBMS listening report), which means that a unicast bearer is needed. The location report from the MC service client is required, since the MC service server must know that the UE has entered a new area and can only listen to MBMS bearer active in that area. If this is not done the MC service server might send a media stream that the MC service client is required to listen to on the MBMS bearer 1, since the MC service server still assumes that the UE is located in the MBSFN area 1.

The solution can be improved as illustrated in figure 10.7.3.7.2-2. In this case two different MBMS bearers are activated (TMGI 1 and TMGI 2), these MBMS bearers are used only for media. An application level signalling bearer is activated (TMGI 9), in both MBSFN areas. This bearer is used for floor control messages and other application level signalling messages that are sent on the MBMS bearer TMGI 9. A similar concept was already introduced in 3GPP TS 23.179 [7] subclause 10.10.2, where the procedure allowed a separate MBMS bearer for floor control signalling. The application level signalling bearer will be used for all control messages needed for both media MBMS bearer (TMGI 1 and TMGI2).

By using an application level signalling bearer (e.g. TMGI 9) the MC service clients can receive floor control messages for all calls going on in the areas of both TMGI 1 and TMGI 2. A MC service client that is located in the area of TMGI 2 and is interested in a MCPTT group call transmission only going on in TMGI 1, can with the information received in TMGI 9 initiate a unicast bearer and request to receive that specific call over a unicast instead. Without the information received over TMGI 9 the MC service client must immediately report that the MC service client has left the broadcast area that the MC service server assumes that the MC service client is located in. With the use of TMGI 9 there is no immediate need for the MC service client to inform the MC service server of a location change.

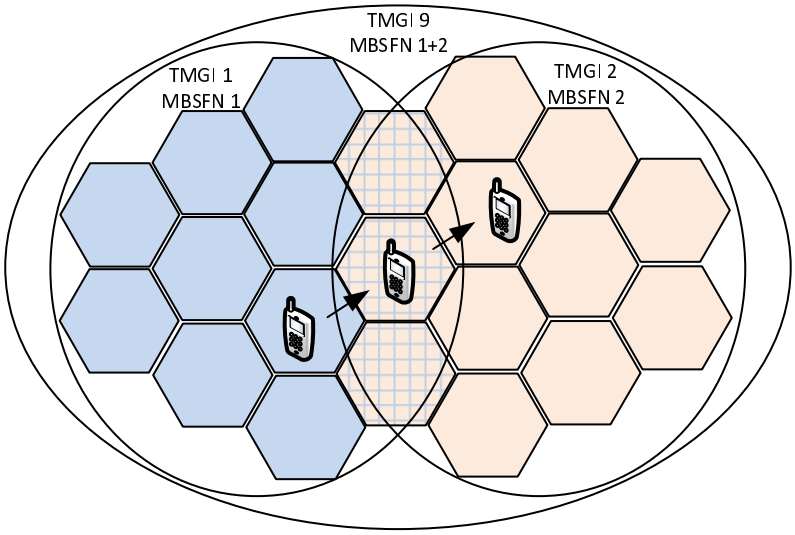

Figure 10.7.3.7.2-2: Two MBMS bearer using overlapping MBSFN areas with a separate MC application signalling bearer

The procedural steps in this scenario will be the same as described above in this subclause. However, in this scenario the MC service client is not required to initiate a unicast bearer to send location report (or MBMS listening report). The UE may move between the two MBMS bearers (TMGI 1 and TMGI 2) without the need to report an area change. A condition for this to work is that there is an application level signalling bearer (TMGI 9) activated in the full area (i.e. the area of both TMGI 1 and TMGI 2). The TMGI 9 will broadcast all floor control messages for all calls ongoing in both areas. If the UE is in coverage of one of the two MBMS bearers that does not transmit the media of interest the UE

can report to the server that it is not able to listen to the media over the MBMS bearer, which triggers the server to use a unicast bearer instead.

10.7.3.7.3 Service continuity with a UE-to-Network relay

This procedure handles a scenario when UE is moving from a location when the UE is experiencing good reception of the MBMS bearer to a location outside the MBMS service coverage. The MC service client apply a service continuity procedure to ensure that the service can be maintained and that the packet loss can be minimized during transition to a UE-to-Network relay connection. The solution also provides the benefit that it offloads the cell when UEs that normally would trigger a transfer from MBMS bearers to unicast bearers when moving outside the MBMS coverage area.

Figure 10.7.3.7.3-1 below illustrates the concept of this procedure. In the figure UE A (with the MC service client) is first within the MBMS coverage (the far right most location). The MBMS coverage is represented by the dashed circle. The UE A is the moving outside the MBMS coverage and first enters a location in which the MBMS signal is not good enough, but in this location there is still coverage to use unicast bearers. Unicast bearers use link adaption and retransmission so the coverage area for unicast bearers is larger than the coverage of the MBMS bearers. The solid circle outer line represents the coverage of the unicast bearer.

A UE that is leaving the area of MBMS coverage may in this scenario trigger a ProSe discovery procedure to initiate the establishment a relay communication path to UE-R. A UE that is receiving media over an MBMS bearer (and is in idle mode) and for the moment does not need a unicast bearer is costly (from a resource efficiency point of view) to transfer to a unicast bearer due to the need for retransmissions and robust coding in the outer part of cell.

When the ProSe communication path is established the UE A may continue to receive the media over the relay UE-R.

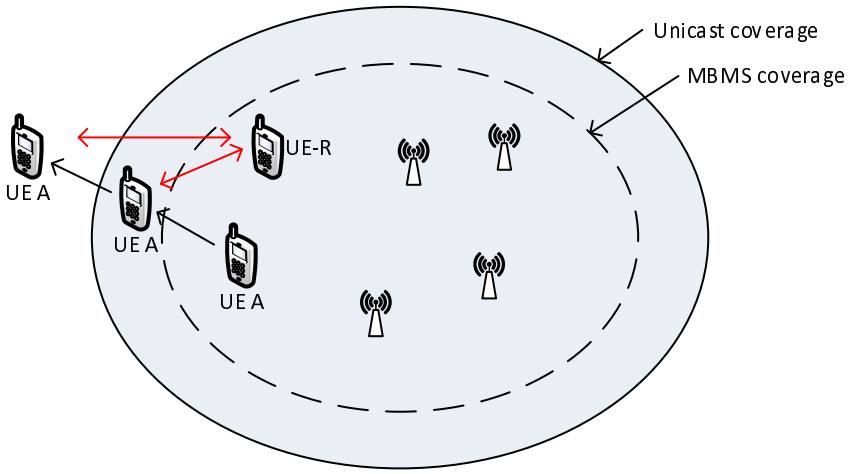

Figure 10.7.3.7.3-1: UE A is moving from a position in MBMS coverage to outside the network coverage passing an area where only unicast is possible

The procedure defined in this subclause allows for MBMS bearer service continuity when UE is moving from a MBMS coverage area to outside the MBMS coverage area. The procedure applies when the UE is not finding a target cell with good RSRP/RSRQ (receiving strong reference signals from other cells), which could trigger normal cell reselection procedure. In such scenario other aspects should be evaluated to trigger to a relay communication path.

Pre-conditions:

- The MC service client UE is not using a unicast bearer when this procedure applies.

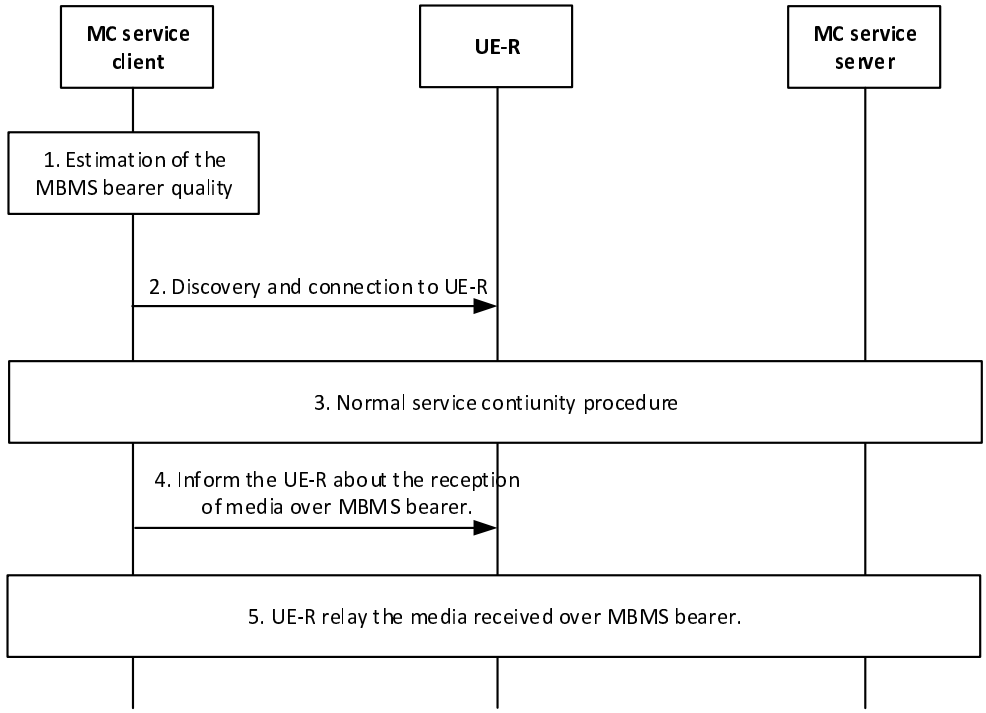

Figure 10.7.3.7.3-2: Service continuity over MBMS bearer using UE-to-network relay

1. The MC service client estimate the MBMS bearer quality. The MC service clients also measure the reference signals from other cells to estimate the possibilities to transfer to unicast and perform a cell reselection procedure.
2. If the MBMS bearer quality has reach a certain threshold the MC service client 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 [14].
3. Normal service continuity procedure for a UE-to-network relay. This may be done according to annex B.
4. The MC service client informs the UE-R about the reception of media over the MBMS bearer. This includes sending the TMGIs, MBMS SAIs and ProSe per packet priority to the UE-R. This procedure is specified in 3GPP TS 23.303 [14].
5. The UE-R will relay the MBMS media using one-to-many ProSe Direct Communication. The UE-R may also relay requests to transfer the media flow from multicast to unicast and vice versa.

10.7.3.8 MBMS suspension notification

10.7.3.8.1 Description

In this procedure the MC sevice client is requested by the MC service server to send a MBMS suspension report. This request for MBMS suspension report can be included in the MBMS bearer announcement and the MC service server may choose to only send this request for MBMS suspension report to a subset of all MC service clients.

10.7.3.8.2 Procedure

The information flow below defines a procedure in which the MC service client notifies the MC service server about an MBMS suspension decision in RAN.

The MC service server can decide on a subset of all UE's in the MBMS broadcast area that shall report on MBMS bearer suspension. When the MC service server make the decision of the UE subset, consideration shall be taken to the

location of the UEs, since UEs location is dynamically changed. This means that the MBMS suspension reporting instruction may need to be updated regularly based on the UEs mobility.

Pre-conditions:

- It is assumed that there is at least one active MBMS bearer

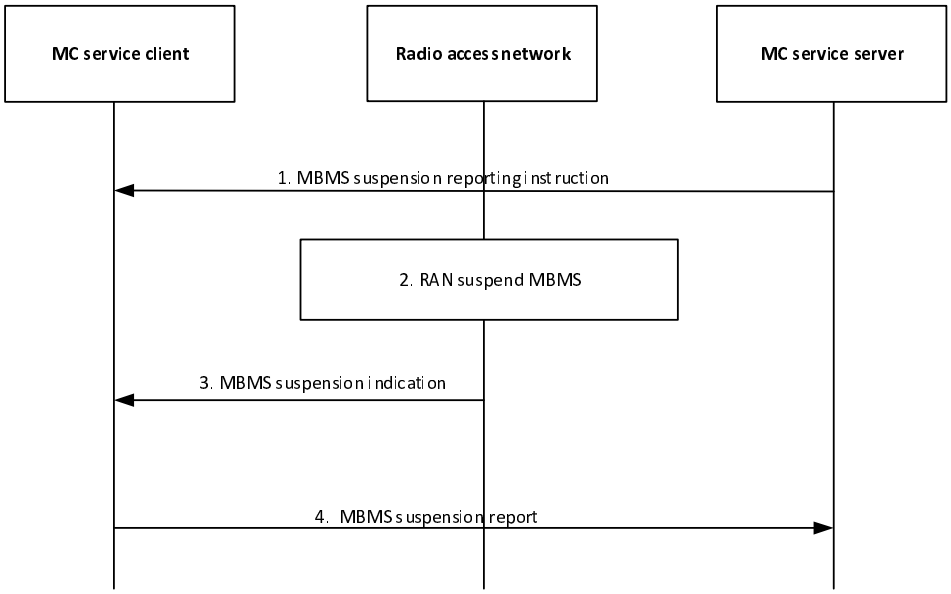

Figure 10.7.3.8.2-1: MBMS suspension notification from MC service client

1. The MC service server sends an MBMS suspension reporting instruction to the MC service client.

NOTE: This message may be included in the MBMS bearer announcement message and may be sent both on a unicast bearer and a multicast bearer.

2. RAN decides to suspend the MBMS bearer, according to existing procedures in 3GPP TS 36.300 [21].

3. An MBMS suspension indication is sent in the MSI (MCH Scheduling Information), according to existing procedures in 3GPP TS 36.300 [21].

4. The MC service client detect the MBMS suspension and sends an MBMS suspension report.

MC service client that is not instructed to send an MBMS suspension report shall still detect the MBMS suspension indication from RAN (step 3). An MC service client shall in this case not send other types of report (e.g. MBMS listening reports).

The same procedure can be applied at MBMS resumption or other MBMS events that may be detected by the MC service client.

10.7.3.9 Multi-server bearer coordination

10.7.3.9.1 General

To avoid allocating duplicate bearers for an MBMS service area, a single MC service server manages all the MBMS media transmission for all groups and users within a particular MBMS service area. An MC service server controlling the MBMS bearer has the MBMS bearer controlling role. Different MC service servers may allocate bearers as needed and make them available for other MC service servers to use.

NOTE: For a single call, multiple MC service servers (participating role) might be involved. Multiple MBMS service areas might have sufficient MC service group members to warrant multiple MBMS bearers to be used and therefore multiple MC service servers (MBMS bearer controlling role) might be involved. For brevity, this clause only illustrates the simplest case.

10.7.3.9.2 Procedures

NOTE 1: This procedure is not fully specified in this version of the document.

Pre-conditions:

- All MC service servers are configured with the contact information of those MC service servers that have, or in the case of dynamic bearer allocation, might make MBMS bearers available for use by other MC service servers.

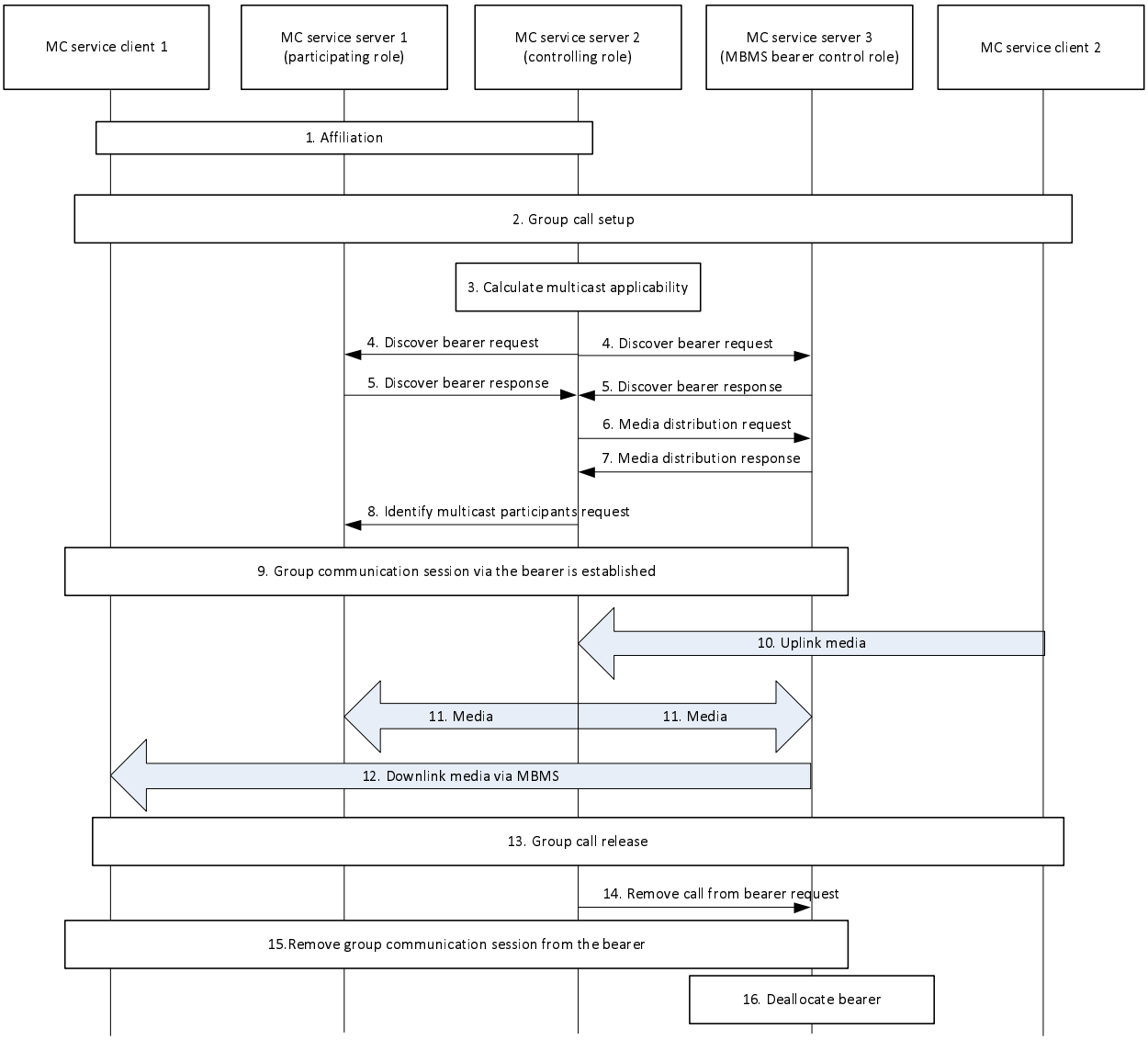

Figure 10.7.3.9.2-1: Multiple server MBMS procedure

1. MC service client 1 affiliates to an MC service group hosted on an MC service server 2 (controlling role) via MC service client 1's MC service server 1 (participating role).

2. MC service client 2 initiates a group call on an MC service group owned by the MC service server 2 (controlling role).

3. The MC service server 2 (controlling role) calculates whether multicast is desired for each service area in which MC service group members are located, based upon the locations, affiliation status and other factors of the MC service group members.

Editor's note: How the MC service server (controlling role) obtains the location information for the MC service clients is FFS.

Editor's note: How the MC service server (controlling role) obtains the listening reports from the MC service clients is FFS.

Editor's note: How the bearer announcement is sent is FFS.

4. The MC service server 2 (controlling role) determines whether another MC service server has already established a bearer with coverage for the MBMS service area where multicast is desired. To do this, the MC service server 2 (controlling role) consults a pre-configured list of MC service servers and sends them a discover bearer request.

NOTE 2: The MC service server which has the MBMS bearer controlling role need not have a participating or controlling role on the call.

NOTE 3: For a single call, multiple MC service servers (participating role) might be involved, multiple MBMS service areas might have sufficient MC service group members to warrant multiple MBMS bearers to be used and therefore multiple MC service servers (in the MBMS bearer controlling role) might be involved. For brevity, this clause only illustrates the simplest case.

NOTE 4: MC service servers of the same type can be configured to discover bearers from a single server. The single server then becomes a centralized MBMS bearer controller for the MC service. Similarly, all MC service servers of all types can be configured to discover bearers from a single server. The single server then becomes a centralized MBMS bearer controller for all MC services.

Editor's note: How the MC service servers identify and route messages to other MC service servers is FFS.

5. The MC service server 3 (MBMS bearer controlling role) responds with a discover bearer response indicating whether there is available bandwidth for the desired bearer. If the bearer of interest has insufficient bandwidth, the polling MC service server 2 may resort to unicast, or may allocate another bearer for the congested area. If a duplicate bearer is allocated for the same area, the bearer should not be shared with other servers and may be torn down as soon as the congestion on the original bearer clears up, in order to conserve resources.

   For any MBMS service areas not covered by another MC service server, the MC service server 2 (controlling role) prepares to distribute media to those MBMS service areas via multicast by setting up a bearer. The bearer set up by the MC service server 2 (controlling role) may then become available for other MC service servers (controlling role) for other MC service groups.

6. The MC service server 2 (controlling role) sends a media distribution request to the MC service server 3 (MBMS bearer controlling role). Information about the call is included so that the MC service server 3 (MBMS bearer controlling role) can send a MapGroupToBearer request on the MBMS bearer to the clients.

7. MC service server 3 (MBMS bearer controlling role) sends a media distribution response to the MC service server 2 (controlling role) indicating whether the request can be supported and supplies details about the bearer.

8. The MC service server 2 (controlling role) informs the MC service server 1 (participating role) of the MC service clients that will be receiving multicast, so that the MC service servers 1 (participating role) need not send via unicast the media to those MC service clients.

9. The MC service server 3 (MBMS bearer controlling role) establishes a group communication session via the bearer, informing MBMS connected MC service clients 1 and 2 that a call is about to start on the MBMS bearer. This step is equivalent to MapGroupToBearer in MCPTT.

10. MC service client 2 sends media on the uplink to the MC service server 2 (controlling role). This step is not dependent upon receipt of the MapGroupToBearer request by MC service client 2.

11. The MC service server 2 (controlling role) forwards the media to MC service server 1 (participating role) so that they can unicast to their affiliated MC service group members that are not MBMS connected or are out of the MBMS service area receiving the broadcast. The MC service server 2 (controlling role) also forwards the media to the MC service server 3 (MBMS bearer controlling role).

12. The MC service server 3 (MBMS bearer controlling role) distributes the media to MBMS served MC service client 1 via multicast.

Editor’s note: Whether the controlling server can send the media directly on MB2U is FFS.

13. At some point later, the group call ends.

14. The MC service server 2 (controlling role) sends a remove call from bearer request, informing the MC service server 3 (MBMB bearer controlling role) to remove the call from the MBMS bearer.

15. The MC service server 3 (MBMS bearer controlling role) removes the group communication session from the bearer. This step is equivalent to UnMapGroupToBearerRequest in MCPTT.

16. The MC service server 3 (MBMS bearer controlling role) may deallocate the MBMS bearer if it has no other calls using the bearer and is configured to allocate and deallocate bearers dynamically as needed.

10.8 Affiliation and de-affiliation to/from MC service group(s)

10.8.1 General

The following subclauses specify the procedures for affiliation and de-affiliation to a single MC service, and which are utilised by the following MC services:

- MCPTT (as specified in 3GPP TS 23.379 [16]);
- MCVideo (as specified in 3GPP TS 23.281 [12]); and
- MCData (as specified in 3GPP TS 23.282 [13]).

MC service specific pre-requisites and resultant behaviour by functional entities in performing these procedures are specified in the respective MC service TSs as listed above.

10.8.2 Information flows

10.8.2.1 MC service group affiliation request

Table 10.8.2.1-1 describes the information flow MC service group affiliation request from the MC service client to the MC service server.

Table 10.8.2.1-1: MC service group affiliation request

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

10.8.2.2 MC service group affiliation request (MC service server – MC service server)

Table 10.8.2.2 -1 describes the information flow MC service group affiliation request between the MC service servers.

Table 10.8.2.2-1: MC service group affiliation request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the MC service group affiliation request.
MC service group ID list	M	A list of one or more MC service group IDs to which the originator intends to affiliate and is defined in the destination MC service system.

10.8.2.3 MC service group affiliation response

Table 10.8.2.3-1 describes the information flow MC service group affiliation response from the MC service server to the MC service client.

Table 10.8.2.3-1: MC service group affiliation response

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

10.8.2.4 MC service group affiliation response (MC service server – MC service server)

Table 10.8.2.4-1 describes the information flow MC service group affiliation response between the MC service servers.

Table 10.8.2.4-1: MC service group affiliation response

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the MC service group affiliation request.
MC service group ID list	M	A list of one or more MC service group IDs to which the originator intends to affiliate and is defined in the destination MC service system.
Affiliation status per MC service group ID	M	Indicates the affiliation result for every MC service group ID in the list.

10.8.2.5 Group affiliation status update

Table 10.8.2.5-1 describes the information flow group affiliation status update from the MC service server to the group management server.

Table 10.8.2.5-1: group affiliation status update

Information element	Status	Description
MC service ID	M	The MC service ID for which the group affiliation status needs to be updated.
MC service group ID list	M	A list of one or more MC service group IDs for which the affiliation status needs to be updated.
Affiliation status per MC service group ID	M	Indicates the affiliation status for every MC service group ID in the list.

10.8.2.6 MC service group de-affiliation request

Table 10.8.2.6-1 describes the information flow MC service group de-affiliation request from the MC service client to the MC service server.

Table 10.8.2.6-1: MC service group de-affiliation request

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

10.8.2.7 MC service group de-affiliation request (MC service server – MC service server)

Table 10.8.2.7-1 describes the information flow MC service group de-affiliation request between the MC service servers.

Table 10.8.2.7-1: MC service group de-affiliation request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the MC service group de-affiliation request.
MC service group ID list	M	A list of one or more MC service group IDs to which the originator intends to de-affiliate and is defined in the destination MC service system.

10.8.2.8 MC service group de-affiliation response

Table 10.8.2.8-1 describes the information flow MC service group de-affiliation response from the MC service server to the MC service client.

Table 10.8.2.8-1: MC service group de-affiliation response

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

10.8.2.9 MC service group de-affiliation response (MC service server – MC service server)

Table 10.8.2.9-1 describes the information flow MC service group de-affiliation response between MC service servers.

Table 10.8.2.9-1: MC service group de-affiliation response

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the MC service group de-affiliation request.
MC service group ID list	M	A list of one or more MC service group IDs to which the originator intends to de-affiliate and is defined in the destination MC service system.
De-affiliation status per MC service group ID	M	Indicates the de-affiliation result for every MC service group ID in the list.

10.8.2.10 Group de-affiliation status update

Table 10.8.2.10-1 describes the information flow group de-affiliation status update from the MC service server to the group management server.

Table 10.8.2.10-1: group de-affiliation status update

Information element	Status	Description
MC service ID	M	The MC service ID for which the group de-affiliation status needs to be updated.
MC service group ID list	M	A list of one or more MC service group IDs for which the de-affiliation status needs to be updated.
De-affiliation status per MC service group ID	M	Indicates the de-affiliation status for every MC service group ID in the list.

10.8.2.11 MC service group affiliation change request

Table 10.8.2.11-1 describes the information flow MC service group affiliation change request from the MC service client to the MC service server.

Table 10.8.2.11-1: MC service group affiliation change request

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the MC service group affiliation change request.
MC service ID list	M	A list of one or more MC service IDs to which the originator intends to the change their MC service group affiliation relationship.
MC service group ID list (per listed MC service ID)	M	A list of one or more MC service group IDs to which the originator intends to change their affiliation relationship with the target user.
Requested affiliation status (per group ID)	M	Indicates if the request is to affiliate or deaffiliate
Change request type	M	Indicates the affiliation request type, i.e. mandatory or negotiated

10.8.2.12 MC service group affiliation change response

Table 10.8.2.12-1 describes the information flow MC service group affiliation change response from the MC service server to the MC service client.

Table 10.8.2.12-1: MC service group affiliation change response

Information element	Status	Description
MC service ID	M	The MC service ID of the originator who triggers the MC service group affiliation request.
MC service ID list	M	A list of one or more MC service IDs to which the originator intends to the change their MC service group affiliation relationship.
MC service group ID list	M	A list of one or more MC service group IDs to which the originator intends to change their affiliation relationship with the target user.
Affiliation status per MC service group ID	M	Indicates the affiliation relationship change result for every MC service group ID in the list.

10.8.3 Affiliation

10.8.3.1 MC service group affiliation procedure

Procedure for affiliation to MC service group(s) for a single MC service is described in figure 10.8.3.1-1.

Pre-conditions:

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

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

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

4. The MC service client triggers the affiliation procedure. This is an explicit affiliation caused either by the MC service user or determined by a trigger event such as the MC service UE coming within a permitted geographic operational area of an MC service group.

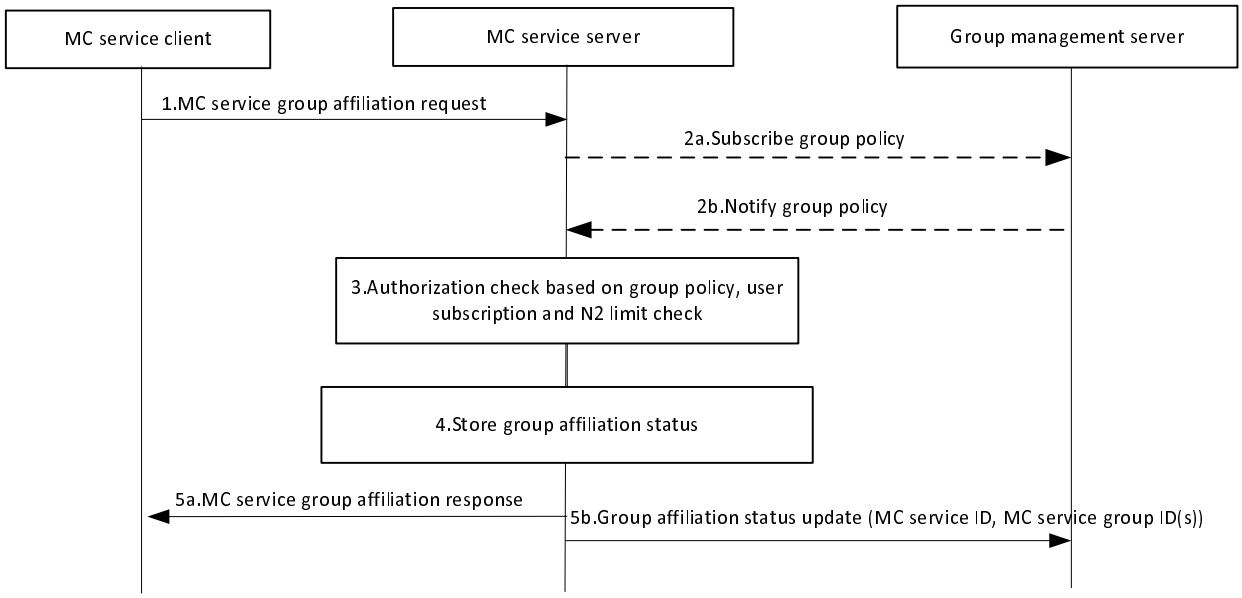

Figure 10.8.3.1-1: MC service group affiliation procedure

1. MC service client of the MC service user requests the MC service server to affiliate to an MC service group or a set of MC service groups.

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

2b. MC service server receives the group policy from the group management server.

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

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

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

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

10.8.3.2 Affiliation to MC service group(s) defined in partner MC service system

10.8.3.2.1 Functional description

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

10.8.3.2.2 Procedure

The procedure for affiliation to MC service group(s) which is defined in a partner MC service system for a single MC service is described in figure 10.8.3.2.2-1.

Pre-conditions:

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

2. The MC service server of the primary MC service system may have locally cached the MC service group affiliation status of the MC service user.

3. The MC service server of the partner MC service system may have retrieved the group related information from the group management server.

4. The MC service client may have indicated to the group management server of the partner MC service system that it wishes to receive updates of group configuration data for MC service group(s) for which it is authorized (as described in subclause 10.1.5.3).

5. The MC service user triggers the affiliation procedure. This is an explicit affiliation caused by the MC service user.

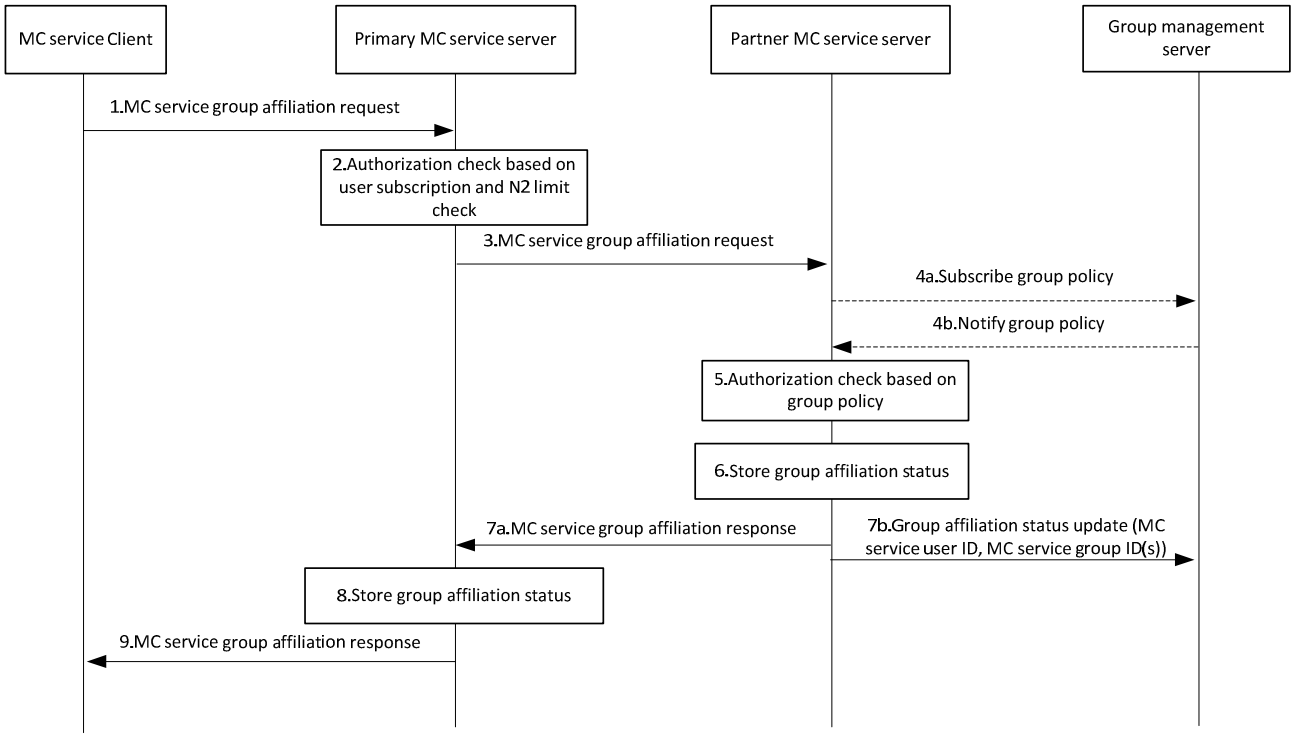

Figure 10.8.3.2.2-1: Affiliation for an MC service group defined in partner MC service system

1. The MC service client requests the MC service server of the primary MC service system to affiliate to an MC service group or a set of MC service groups.

2. The MC service server of the primary MC service system checks if the MC service client is authorized to affiliate to the requested MC service group(s) based on the user subscription. The MC service server also performs the check for the maximum limit of the total number (N2) of MC service groups that the user can be affiliated to simultaneously.

3. Based on the group information included in the request, the MC service server of the primary MC service system, it determines to send group affiliation request to the corresponding MC service server of the partner MC service system. The request may be routed through intermediate signalling nodes.

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

4b. The MC service server of the partner MC service 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 MC service server of the partner MC service system checks if the MC service group(s) is not disabled and if the user of the MC service client is authorised to affiliate to the requested MC service group(s).

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

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

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

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

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

10.8.4 De-affiliation from MC service group(s)

10.8.4.1 General

When an MC service user does not want to communicate with an MC service group anymore for a single MC service, then the MC service user can revoke its affiliation to the MC service group.

10.8.4.2 MC service group de-affiliation procedure

The procedure for revoking the affiliation with an MC service group for a single MC service is described in figure 10.8.4.2-1.

Pre-conditions:

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

2. The MC service client triggers the de-affiliation procedure. This is an explicit de-affiliation requested either by the MC service user or determined by a trigger event such as the MC service UE moving outside a permitted geographic operational area of an MC service group.

NOTE: The geographical operational area beyond which de-affiliation occurs may be larger than the geographical operational area within which affiliation is permitted, to avoid repeated affiliation and de-affiliation by a user on the edge of an operational area.

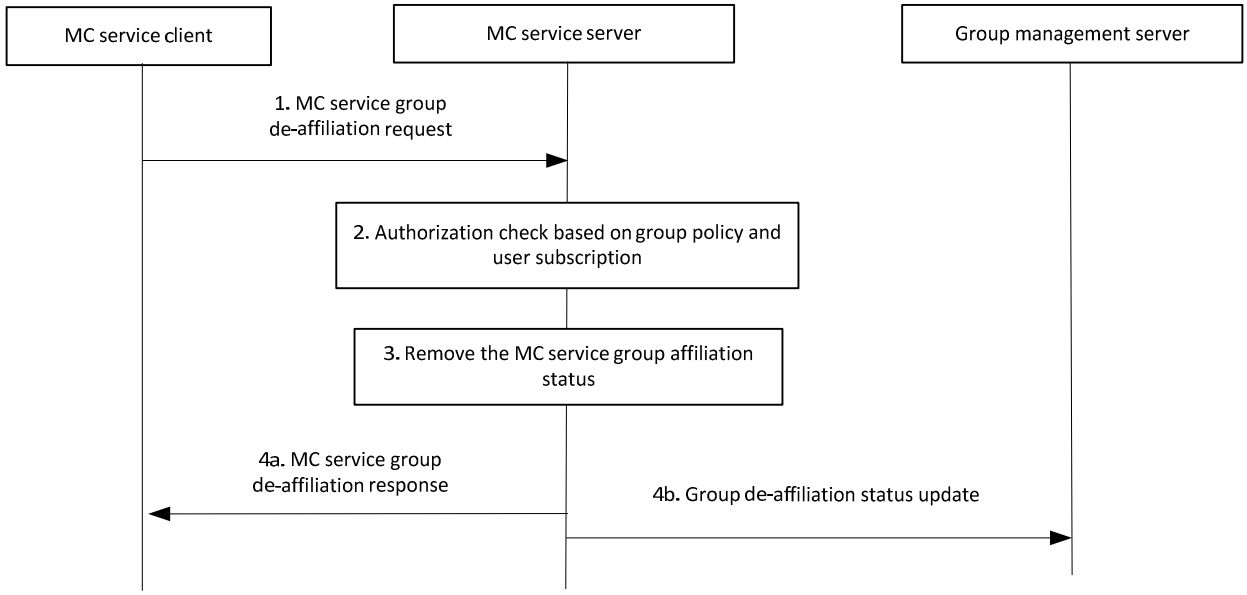

Figure 10.8.4.2-1: MC service group de-affiliation procedure

1. MC service client requests the MC service server to de-affiliate from an MC service group or a set of MC service groups.

2. Based on the user subscription and stored group policy, the MC service server checks if the user of the MC service client is authorized to de-affiliate from the requested MC service group(s) and if the user of the MC service client has affiliated to the requested MC service group(s).

3. If the user of the MC service client has affiliated to the requested MC service group(s), is authorized to de-affiliate from the requested MC service group(s) then the MC service server removes the affiliation status of the user for the requested MC service group(s).

4. MC service server provides to the MC service client the group de-affiliation response (4a) and updates the group management server with the de-affiliation status of the user for the requested MC service group(s) (4b).

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

10.8.4.3 De-affiliation from MC service group(s) defined in partner MC service system

The procedure for de-affiliation from affiliated MC service group(s) which is defined in partner MC service system for a single MC service is described in figure 10.8.4.3-1.

Pre-conditions:

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

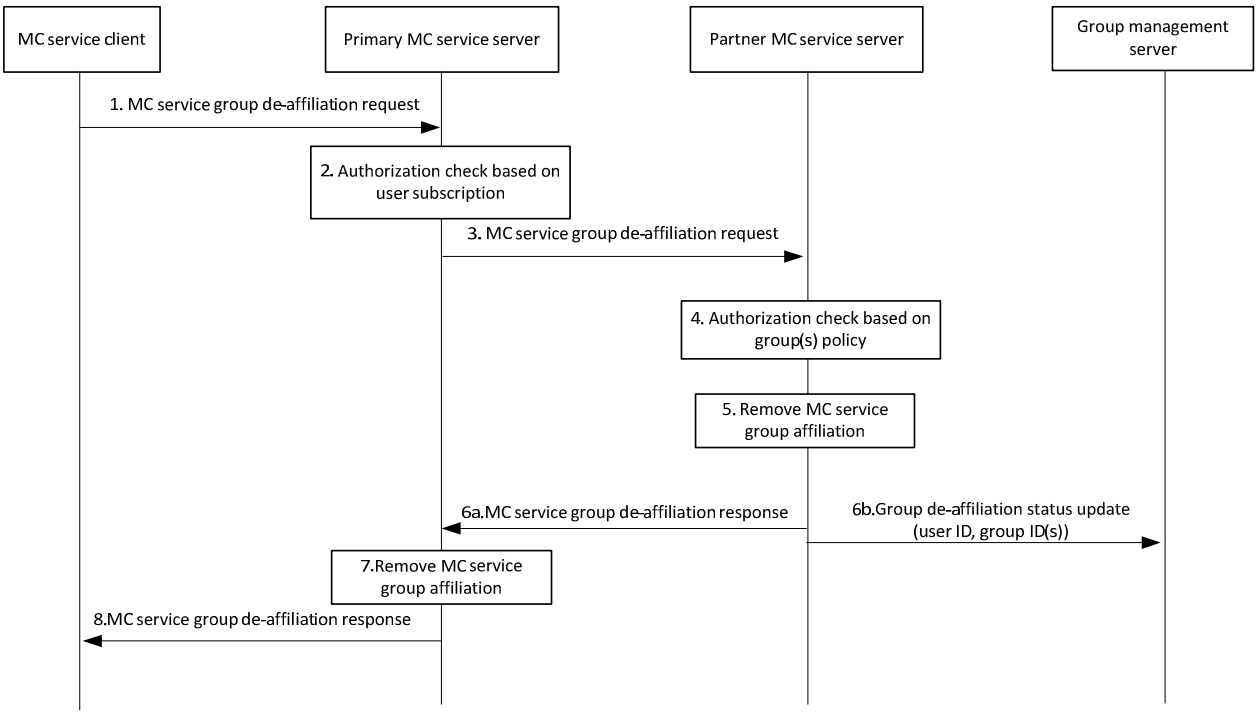

Figure 10.8.4.3-1: De-affiliation from an MC service group defined in partner MC service system

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

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

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

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

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

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

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

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

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

10.8.5 Remote change of affiliation

10.8.5.1 Remote change of affiliation for groups defined in primary MC service system

10.8.5.1.1 Authorized user remotely changes another MC service user's affiliated MC service group(s) – mandatory mode

The procedure for an authorized user to remotely change another MC service user's affiliated MC service group(s) for a single MC service without requiring the target user's approval is described in figure 10.8.5.1.1-1.

Pre-conditions:

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

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

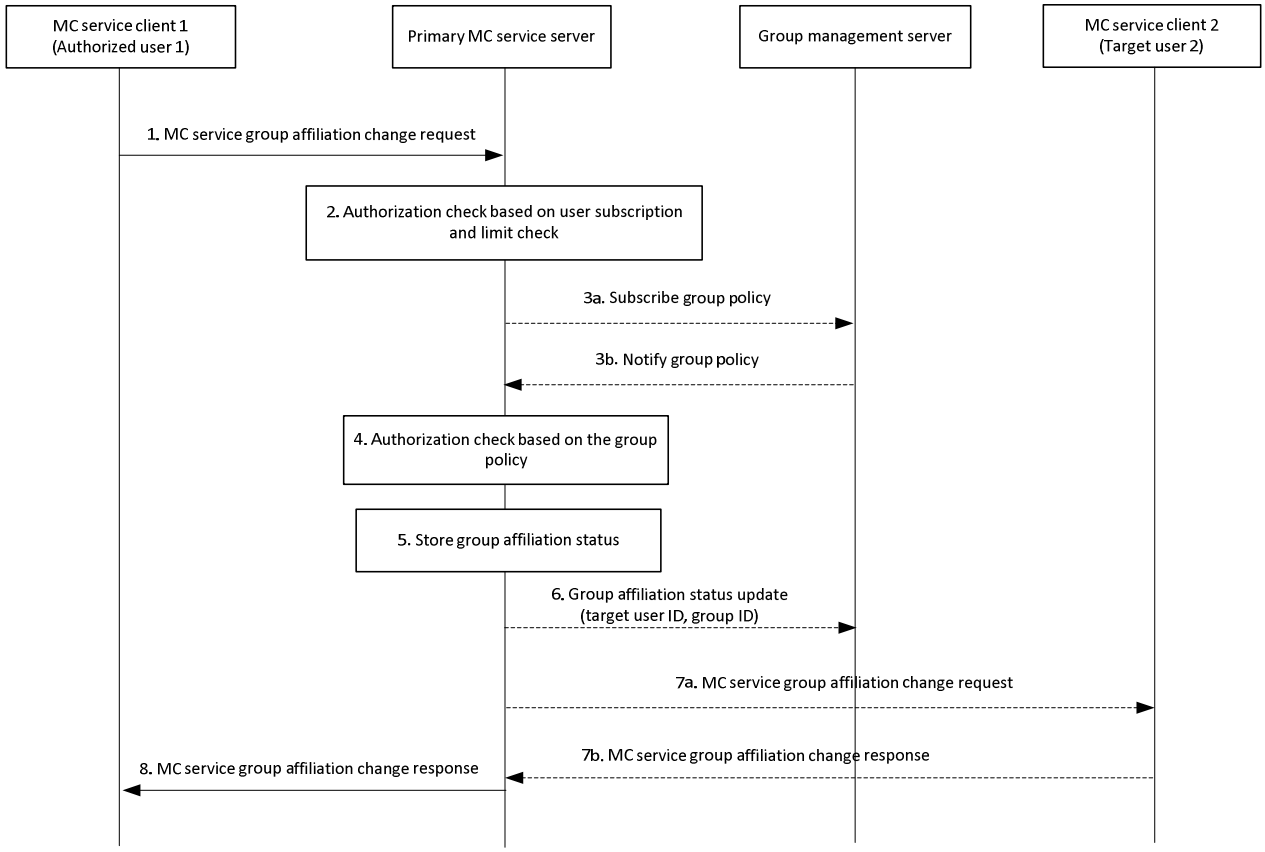

Figure 10.8.5.1.1-1: Remotely change MC service group affiliation – mandatory mode

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

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

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

3b. The primary MC service 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 MC service server checks if the target MC service user 2 is authorized to affiliate or de-affiliate to the MC service group(s).

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

6. If the requested affiliation status is a change from the current affiliation status, then the primary MC service server updates the group management server with the affiliation status of the MC service user 2 for the MC service group(s).

7a. If the requested affiliation status is a change the primary MC service server sends the MC service group affiliation change request with the indication of mandatory mode to MC service client 2 of the target MC service user 2. The target MC service user 2 receives the latest information about the affiliated MC service groups. The

MC service client 2 may subscribe to the affiliated MC service groups information with the group management server.

7b. The MC service user 2 provides a response to the primary MC service server by sending an MC service group affiliation change response.

8. The primary MC service server sends the MC service group affiliation change response to MC service client 1. If the requested affiliation status was not changed (see 7a), then the MC service server creates an appropriate (accept) MC service group affiliation change response to send to MC service client 1.

NOTE: Steps 6, 7a, 7b and 8 can occur in any order or in parallel, with the restriction that step 7b can only occur after step 7a occurred.

10.8.5.1.2 Authorized user remotely changes another MC service user's affiliated MC service group(s) – negotiated mode

The procedure for the authorized user to remotely change another MC service user's affiliated MC service group(s) for a single MC service with the target MC service user's approval is described in figure 10.8.5.1.2-1.

Pre-conditions:

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

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

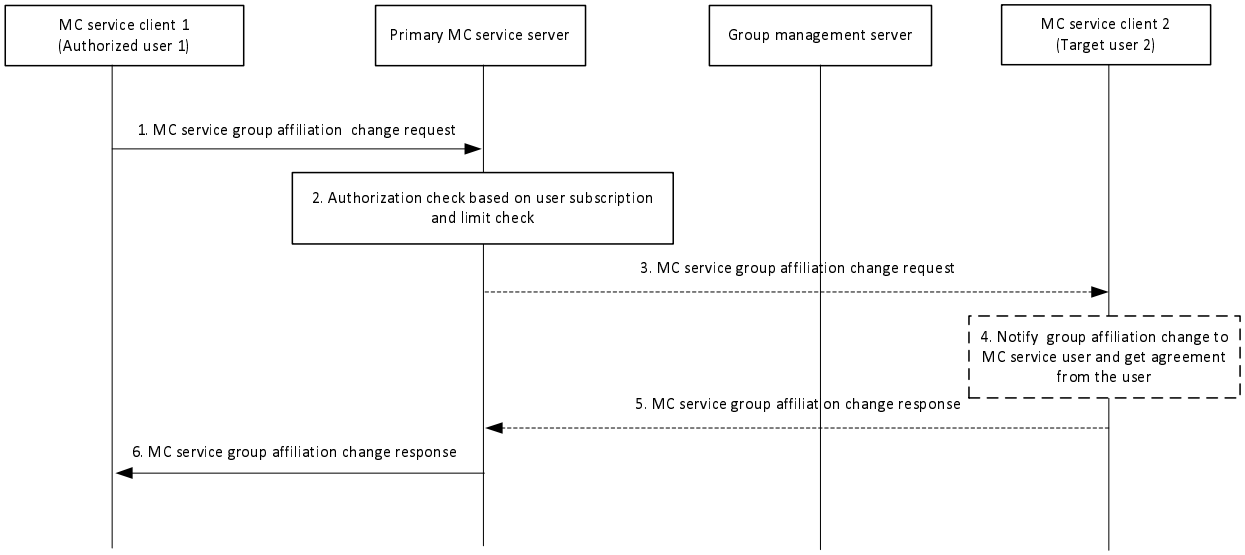

Figure 10.8.5.1.2-1: Remotely change MC service group affiliation – negotiated mode

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

2. The primary MC service server checks if the MC service user 1 is authorized to initiate the change of the affiliation relationship between the target user 2 and the MC service group(s). The primary MC service server checks if the target MC service user(s) are authorized for the requested affiliation relationship based on the user subscription and the group policy (i.e. if not available, the primary MC service server obtains the group policy from the group management server). The primary MC service server also performs the check for the maximum limit on the total number (N2) of MC service groups that the user can be affiliated to simultaneously.

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

4. If the requested affiliation status is different from the current affiliation status, then the MC service client 2 notifies the MC service group affiliation change request to the target MC service user 2 to receive the approval from the user on the proposed changes to the affiliated MC service group(s).

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

5. If the target MC service user 2 provides a response (accept or reject) to the notification, then the MC service client 2 sends an MC service group affiliation change response to the primary MC service server. A 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 MC service server (see subclause 10.8.3.1 or subclause 10.8.4.2) as per the MC service 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 MC service groups defined in partner MC service systems, the primary MC service server performs the affiliation or de-affiliation procedures by interacting with the partner MC service systems (see subclause 10.8.3.2 or subclause 10.8.4.3).

6. The primary MC service server sends the MC service group affiliation change response to the MC service client 1. If the requested affiliation status was not changed (see 4), then the MC service server creates an appropriate (accept) MC service group affiliation change response to send to MC service client 1.

NOTE 3: If multiple MC service groups are included in step 1, and these MC service groups belong to different partner MC service systems, the primary MC service server can wait until all the partner MC service systems provides the MC service group affiliation change response messages.

10.8.5.2 Remote change of affiliation for groups defined in partner MC service system

10.8.5.2.1 Authorized user remotely changes another MC service user's affiliated MC service group(s) defined in partner MC service system – mandatory mode

The procedure for the authorized user to remotely change another MC service user's affiliated MC service group(s) defined in partner MC service systems for a single MC service without requiring the target user's approval is described in figure 10.8.5.2.1-1.

Pre-conditions:

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

- The MC service client 1 (authorized user 1), MC service client 2 (target MC service user 2), and the primary MC service server belong to the same MC service system;

- The partner MC service server may have retrieved the group related information from the group management server; and

- The primary MC service server may have retrieved the user policy e.g. user related information regarding user(s) authorization to affiliate or to de-affiliate to MC service group(s), priority, and other related configuration data.

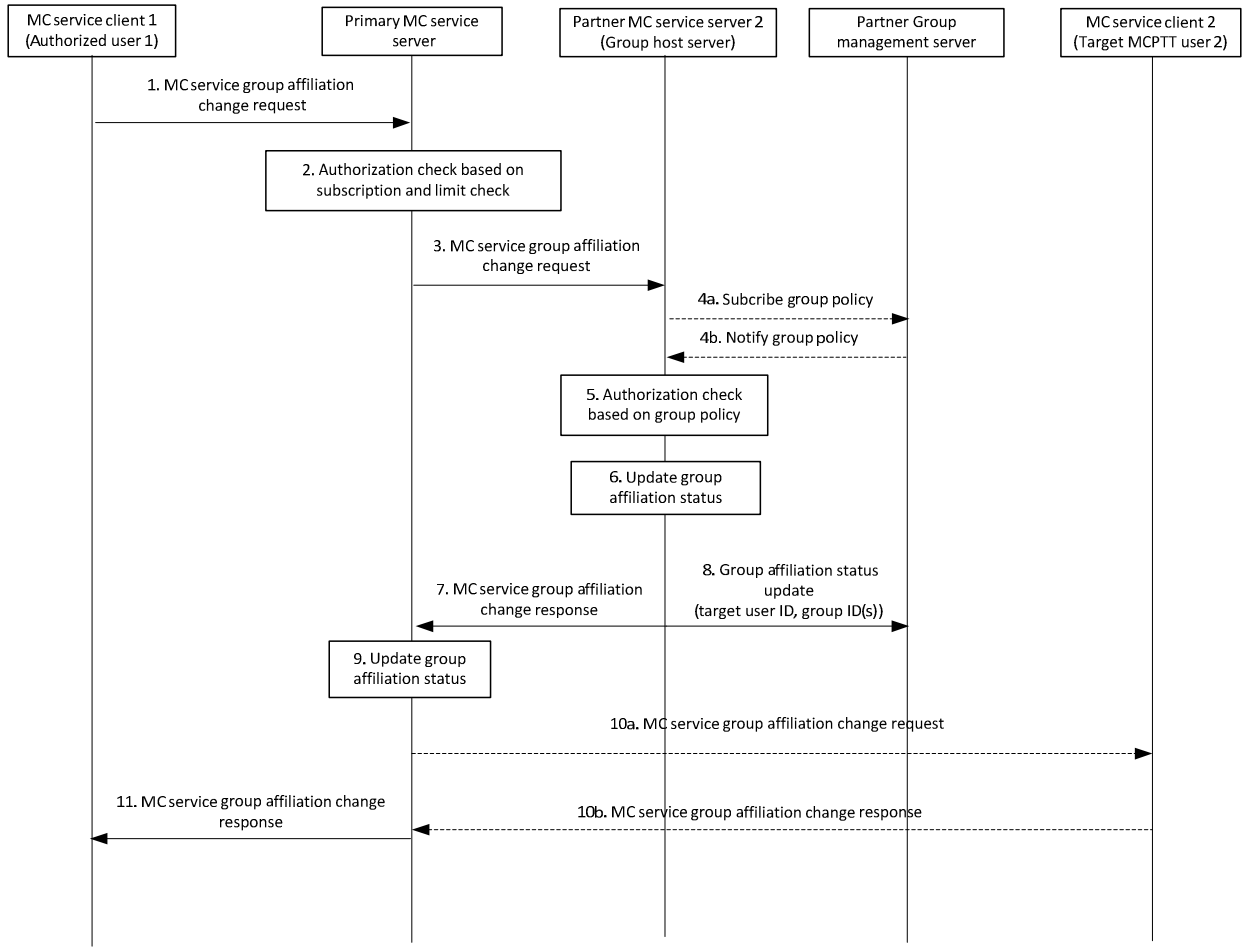

Figure 10.8.5.2.1-1: Remote change MC service group affiliation defined in partner MC service system – mandatory mode

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

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

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

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

4b. The partner MC service 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 MC service server checks if the target MC service user 2 is authorized to affiliate to the MC service group(s). It is possible that the target MC service user 2 affiliates to one or more MC service groups and also de-affiliates from one or more MC service groups.

6. If the target MC service user 2 is authorized to affiliate or de-affiliate to the MC service group(s) and if the requested affiliation status is different to the current affiliation status, then the partner MC service server stores the new affiliation status of the target MC service user 2 for the MC service group(s).

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

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

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

9. If the requested affiliation status is different to the current affiliation status, then the primary MC service server stores the new affiliation status of the target MC service user 2 for the MC service group(s).

10a. If the requested affiliation status is different to the current affiliation status, then the primary MC service server sends the MC service group affiliation change request with the indication of mandatory mode to MC service client 2 of the target MC service user 2. The target MC service user 2 receives the latest information about the affiliated MC service groups. Further the MC service client 2 may subscribe for the affiliated MC service groups information with the group management server.

10b. The target MC service client 2 provides an MC service group affiliation change response to the MC service server.

11. The primary MC service server sends the MC service group affiliation change response to MC service client 1 (authorized user). If the requested affiliation status was not changed (see 10a), then the MC service server creates an appropriate (accept) MC service group affiliation change response to send to MC service client 1.

10.9 Location management (on-network)

10.9.1 General

Location information of MC service user shall be provided by the location management client to the location management server. The location information reporting triggers are based on the location reporting configuration. Different type of location information can be provided.

10.9.2 Information flows for location information

10.9.2.1 Location reporting configuration

Table 10.9.2.1-1 describes the information flow from the location management server to the location management client for the location reporting configuration.

Table 10.9.2.1-1: Location reporting configuration

Information element	Status	Description
MC service ID	M	Identity of the MC service user to which the location reporting configuration is targeted.
Requested non-emergency location information	O (NOTE)	Identifies what location information is requested, except for emergency or imminent peril calls or emergency alerts
Requested emergency location information	O (NOTE)	Identifies what location information is requested, for emergency or imminent peril calls or emergency alerts
Triggering criteria in non-emergency cases	O (NOTE)	Identifies when the location management client will send the location report in non-emergency cases
Minimum time between consecutive reports	O (NOTE)	Defaults to 0 if absent and 0 for emergency calls, imminent peril calls and emergency alerts
NOTE: If none of the information element is present, this represents a cancellation for location reporting.		

10.9.2.2 Location information report

Table 10.9.2.2-1 describes the information flow from the location management client to the location management server for the location information reporting.

Table 10.9.2.2-1: Location information report

Information element	Status	Description
Set of MC service IDs	M	Set of identities of the reporting MC service user on the MC service UE (e.g. MCPTT ID, MCVideo ID, MCData ID)
Triggering event	M	Identity of the event that triggered the sending of the report
Location Information	M	Location information

10.9.2.3 Location information request

Table 10.9.2.3-1 describes the information flow from the MC service server to the location management server and from the location management server to the location management client for requesting an immediate location information report.

Table 10.9.2.3-1: Location information request

Information element	Status	Description
MC service ID list	M	List of MC service users whose location information is requested

10.9.2.4 Location reporting trigger

Table 10.9.2.4-1 describes the information flow from the location management client to the location management server for triggering a location reporting procedure.

Table 10.9.2.4-1: Location reporting trigger

Information element	Status	Description
MC service ID	M (NOTE 1)	Identity of the requesting authorized MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
MC service ID	M (NOTE 1)	Identity of the requested MC service user (e.g. MCPTT ID, MCVideo ID, MCData ID)
Immediate Report Indicator	O (NOTE 2)	Indicates whether an immediate location report is required
Requested non-emergency location information	O (NOTE 2)	Identifies what location information is requested, except for emergency or imminent peril calls or emergency alerts
Requested emergency location information	O (NOTE 2)	Identifies what location information is requested, for emergency or imminent peril calls or emergency alerts
Triggering criteria in non-emergency cases	O (NOTE 2)	Identifies when the client will send the location report in non-emergency cases
Minimum time between consecutive reports	O (NOTE 2)	Defaults to 0 if absent and 0 for emergency calls, imminent peril calls and emergency alerts
NOTE 1: The identity of the requesting MC service user and the requested MC service user should belong to the same MC service. E.g. if requesting MC service user is using a MCPTT ID, then the requested MC service user identity should be an MCPTT ID. NOTE 2: At least one of these rows shall be present.		

10.9.2.5 Location information subscription request

Table 10.9.2.5-1 describes the information flow from the MC service server to the location management server for location information subscription request.

Table 10.9.2.5-1: Location information subscription request

Information element	Status	Description
MC service ID	M	Identity of the requesting MC service user
MC service ID list	M	List of MC service users whose location information is requested.
Time between consecutive reports	M	It indicates the interval time between consecutive reports

10.9.2.6 Location information subscription response

Table 10.9.2.6-1 describes the information flow from the location management server to the MC service server for location information subscription response.

Table 10.9.2.6-1: Location information subscription response

Information element	Status	Description
MC service ID	M	Identity of the requesting MC service user
Subscription status	M	It indicates the subscription result

10.9.2.7 Location information notification

Table 10.9.2.7-1 describes the information flow from the location management server to the MC service server.

Table 10.9.2.7-1: Location information notification

Information element	Status	Description
MC service ID list	M	List of the MC service users whose location information needs to be notified
MC service ID	M	Identity of the MC service user subscribed to location of another MC service user (NOTE)
Triggering event	M	Identity of the event that triggered the sending of the notification
Location Information	M	Location information
NOTE: This is only used for location management server sends location information notification to the MC service user who has subscribed the location.		

10.9.3 Procedure

10.9.3.1 Event-triggered location reporting procedure

The location management server provides location reporting configuration to the location management clients, indicating what information the location management server expects and what events will trigger the sending of this information to the location management server. The decision to report location information can be triggered at the location management client by different conditions, e.g., the reception of the location reporting configuration, initial registration, distance travelled, elapsed time, cell change, MBMS SAI change, MBMS session change, leaving a specific MBMS bearer service area, tracking area change, PLMN change, call initiation, or other types of events such as emergency alert, emergency call or imminent peril calls. The location report can include information described as ECGI, MBMS SAIs, geographic coordinates and other location information.

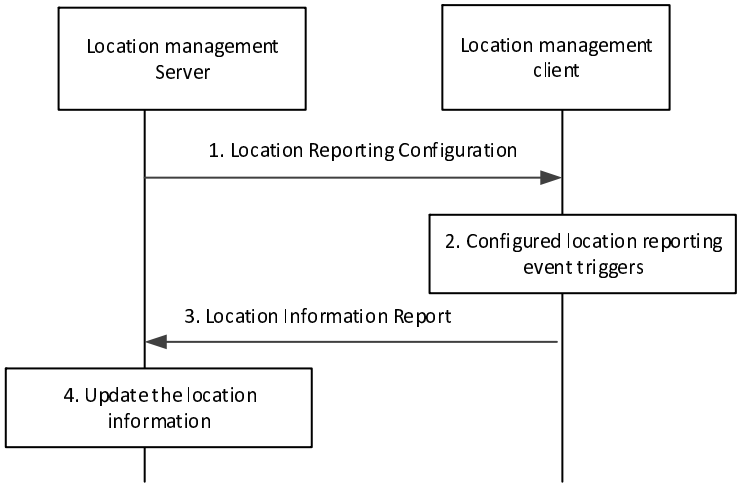

Figure 10.9.3.1-1: Event-triggered location reporting procedure

1. The MC service server sends location reporting configuration message to the MC service client(s) containing the initial configuration (or a subsequent update) for reporting the location of the MC service UE. This message can be sent over a unicast bearer to a specific MC service client or as a group message over an MBMS bearer to update the location reporting configuration for multiple MC service clients at the same time.

NOTE 1: The location reporting configuration information can be made part of the user profile, in which case the sending of the message is not necessary.

NOTE 2: Different location management clients may be given different location reporting criteria.

2. A location reporting event occurs, triggering step 3.

3. The location management client sends a location information report to the location management server, containing location information identified by the location management server and available to the location management client.

4. Upon receiving the report, the location management server updates location of the reporting location management client. If the location management server does not have location information of the reporting location management client before, then just stores the reporting location information for that location management client.

10.9.3.2 On-demand location reporting procedure

The location management server can request UE location information at any time by sending a location information request to the location management client, which may trigger location management client to immediately send the location report.

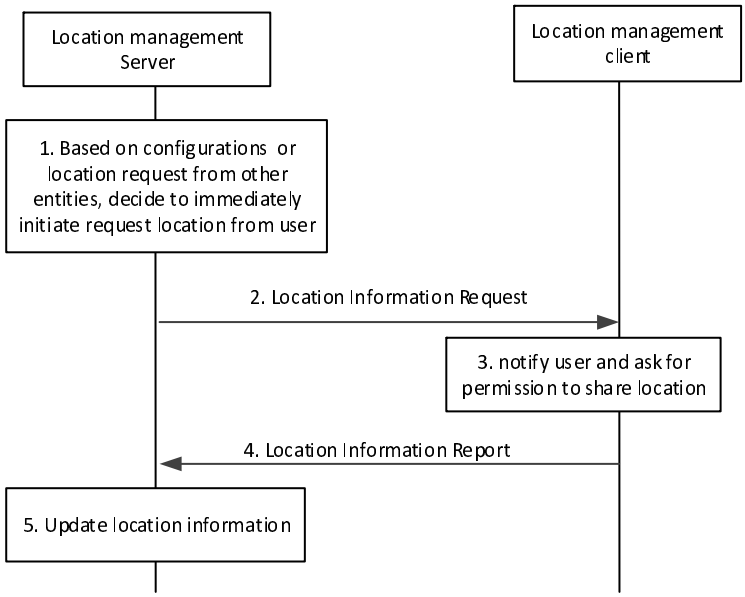

Figure 10.9.3.2-1: On-demand location information reporting procedure

1. Based on configurations such as periodical location information timer, or location information request from other entities (e.g., another location management client, MC service server), location management server initiates the immediately request location information from the location management client.

2. The location management server sends a location information request to the location management client.

3. MC service user is notified and asked about the permission to share its location. MC service user can accept or deny the request

4. The location management client immediately responds to the location management server with a report containing location information identified by the location management server and available to the location management client.

5. Upon receiving the report, the location management server updates location of the reporting location management client. If the location management server does not have location information of the reporting location management client before, then just stores the reporting location information for that location management client.

10.9.3.3 Client-triggered location reporting procedure

Figure 10.9.3.3-1 illustrates the high level procedure of client-triggered location reporting.

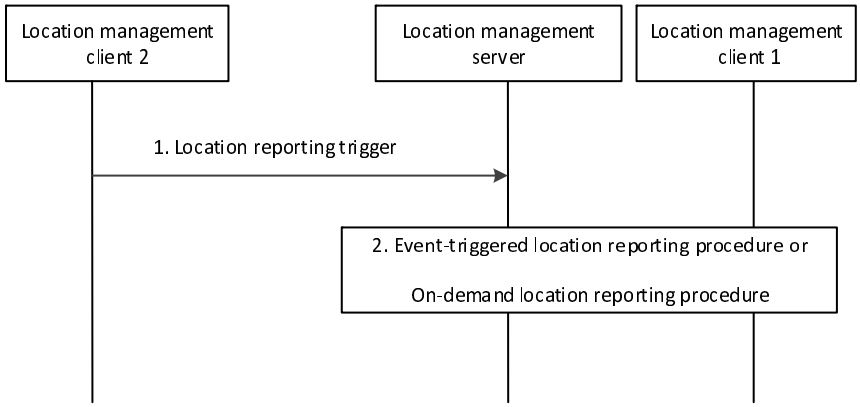

Figure 10.9.3.3-1: Client-triggered location reporting procedure

1. Location management client 2 (authorized MC service user) sends a location reporting trigger to the location management server to activate a location reporting procedure for obtaining the location information of location management client 1.
2. Location management server checks whether location management client 2 is authorized to send a location reporting trigger. Depending on the information specified by the location reporting trigger, location management server initiates an on-demand location reporting procedure or an event-triggered location reporting procedure for the location of location management client 1.

10.9.3.4 Location reporting cancel procedure

The location reporting cancel procedure reuses the information flow of location reporting configuration.

Pre-conditions:

- The location management client has been provided the location reporting configuration information.

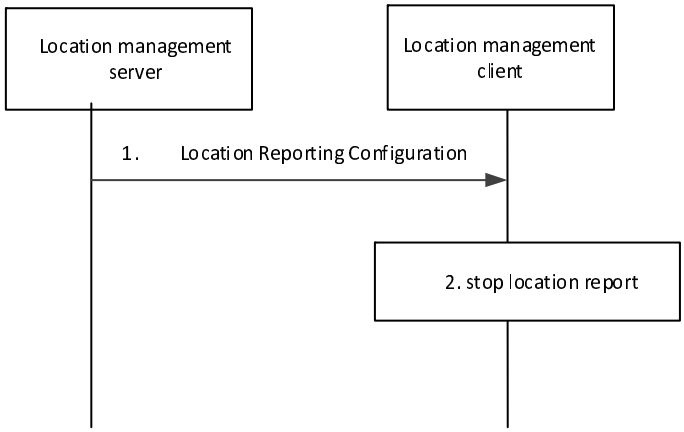

Figure 10.9.3.4-1: Location reporting cancel procedure

1. The location management server sends location reporting configuration without any information element to the location management client to stop location reporting from the MC service UE.
2. The location management client stops sending location information reports to the location management server.

10.9.3.5 Location information subscription procedure

Figure 10.9.3.5-1 illustrates the high level procedure of location information subscription request. The same procedure can be applied for location management client and other entities that would like to subscribe to MC service user location information.

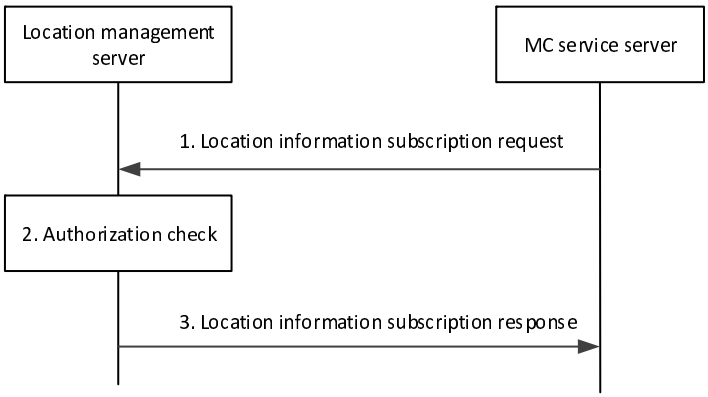

Figure 10.9.3.5-1: Location information subscription request procedure

1. MC service server sends a location information subscription request to the location management server to subscribe location information of one or more MC service users.
2. The location management server shall check if the MC service server is authorized to initiate the location information subscription request.
3. The location management server replies with a location information subscription response indicating the subscription status.

10.9.3.6 Usage of location information procedure

10.9.3.6.1 Event-trigger location information notification procedure

Figure 10.9.3.6.1-1 illustrates the high level procedure of event-trigger usage of location information. The same procedure can be applied for location management client and other entities that would like to subscribe to location information of MC service user.

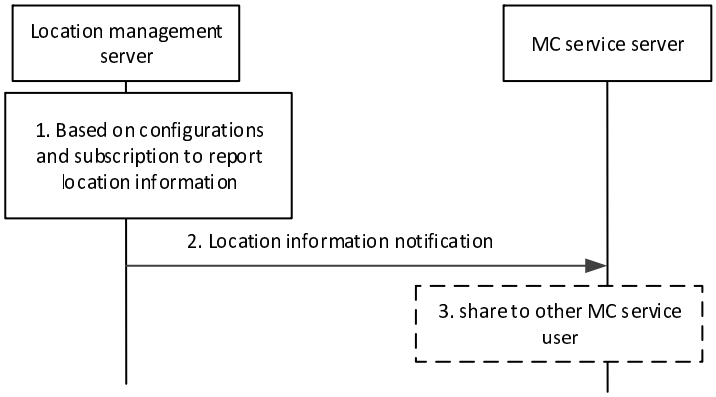

Figure 10.9.3.6.1-1: Event-trigger usage of location information procedure

1. Based on the configurations, e.g., subscription, periodical location information timer, location management server is triggered to report the latest user location information to MC service server.

2. The location management server send the location information report including the latest location information of one or more MC service users to the MC service server. The latest location information is from the location report procedure as described in subclause 10.9.3.1, or from PLMN operator.

3. MC service server may further share this location information to a group or to another MC service user.

NOTE: For other entities, the step 3 can be skipped if not needed.

10.9.3.6.2 On-demand usage of location information procedure

The MC service server can request UE location information at any time by sending a location information request to the location management server, which may trigger location management server to immediately send the location report.

Figure 10.9.3.6.2-1 illustrates the high level procedure of on demand usage of location information. The same procedure can be applied for location management client and other entities that would like to subscribe to location information of MC service user.

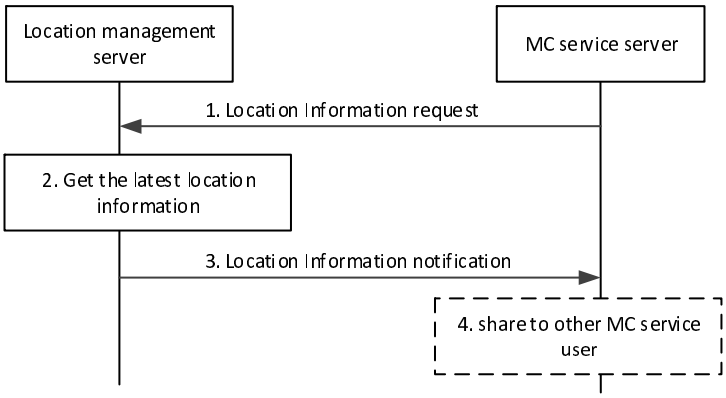

Figure 10.9.3.6.2-1: On-demand usage of location information procedure

1. MC service server sends a location information request to the location management server.

2. The location management server acquires the latest location of the UEs being requested, by triggering an on-demand location report procedure as described in subclause 10.9.3.2, or from PLMN operator.

3. Then, location management server immediately sends the location information report including the latest location information acquired of one or more MC service users.

4. MC service server may further share this location information to a group or to another MC service user.

NOTE: For other entities, the step 3 can be skipped if not needed.

10.10 Emergency Alert

10.10.1 On-network emergency alert

10.10.1.1 General

The following subclauses specify the procedures for emergency alert initiation and emergency state cancel that are utilised by the following MC services:

- MCVideo service
- MCData service

Editor's note: Whether the following procedures for emergency alert initiation and emergency state cancel apply to MCPTT service also is FFS.

10.10.1.2 MC service emergency alert

10.10.1.2.1 MC service emergency alert initiation

The procedure focuses on the case where an MC service client is initiating an MC service emergency alert unicast signalling for communicating the alert with the affiliated MC service group members of that MC service group. An MC service client in the MC service emergency state gains elevated access privilege for all of the MC service user's mission critical applications. This procedure will place the MC service client in the MC service emergency state if the MC service client is not already in that state.

Procedures in figure 10.10.1.2.1-1 are the signalling control plane procedures for the MC service client initiating an MC service emergency alert with an MC service group i.e., MC service users on MC service client 1, MC service client 2 and MC service client 3 belong to the same MC service group which is defined on group management server.

NOTE 1: For simplicity, a single MC service server is shown in place of a user home MC service server and a group hosting MC service server.

Pre-conditions:

1. The MC service group is previously defined on the group management server with MC service client 2 and MC service client 3 affiliated to that MC service group.
2. All members of the MC service group belong to the same MC system.
3. The initiating MC service client 1 is affiliated with one or more MC service groups.
4. The initiating MC service client 1 has been provisioned with an MC service group designated as the MC service emergency group.

NOTE 2: Alternatively, the client could have been provisioned for emergency behaviour on the currently selected group.

5. The initiating MC service client 1 may not have carried out an explicit affiliation procedure with the MC service group designated as the MC service emergency group.

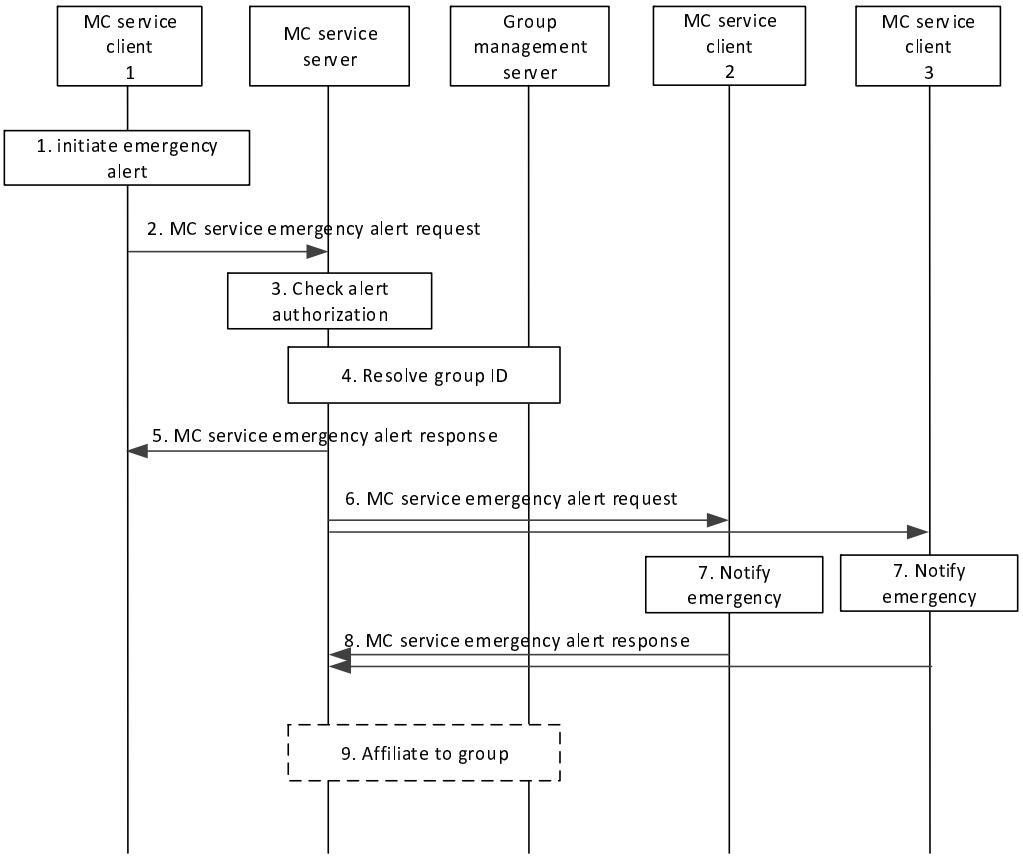

Figure 10.10.1.2.1-1 MC service emergency alert

1. The user at the MC service client 1 initiates an MC service emergency alert. MC service client 1 sets its MC service emergency state. The MC service emergency state is retained by the MC service client until explicitly cancelled.

2. MC service client 1 requests the MC service server to send an MC service emergency alert request to the MC service group designated as the MC service emergency group.

3. MC service server checks whether the MC service user of MC service client 1 is authorized for initiation of MC service emergency alerts for the indicated MC service group.

4. MC service server resolves the MC service group ID to determine the members of that MC service group and their affiliation status, based on the information from group management server.

5. The MC service server sends the MC service emergency alert response to the MC service user 1 to confirm the MC service emergency alert request. MC service group calls made to this MC service group by the MC service client 1 will be sent as emergency calls until the emergency state on the MC service client 1 is cancelled.

6. The MC service server sends an MC service emergency alert request towards the MC service clients of each of those affiliated MC service group members. The MC service emergency alert request message shall contain the following information: Location, MC service ID and MC service group ID (i.e., MC service user's selected MC service group or dedicated MC service emergency group, as per MC service group configuration) and the MC service user's mission critical organization name.

7. MC service users are notified of the MC service emergency.

8. The receiving MC service clients send the MC service emergency alert response to the MC service server to acknowledge the MC service emergency alert.

9. The MC service 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 MC service client 1 need not initiate a group call. For example, the MC service client can be configured to only allow alerts or the MC service user can choose not to make an MC service emergency group call.

Editor's note: How emergency alert is synchronized between MC services is FFS.

10.10.1.2.2 MC service emergency state cancel

The procedure focuses on the case where an MC service client has initiated an MC service emergency alert and entered the emergency state, and wishes to cancel this state, informing the MC service server and other group members of this cancellation. By doing so, the MC service client may also request the cancellation of the ongoing emergency condition in the group.

Procedures in figure 10.10.1.2.2-1 are the signalling control plane procedures for the MC service client cancelling an MC service emergency state with an MC service group i.e., MC service users on MC service client 1, MC service client 2 and MC service client 3 belong to the same MC service group which is defined on MC service group management server.

NOTE 1: For simplicity, a single MC service server is shown in place of a user home MC service server and a group hosting MC service server.

Pre-conditions:

1. The MC service client 1 had previously successfully initiated an MC service emergency alert.
2. The MC service client 1 is still in the emergency state.
3. The initiating MC service client 1 has affiliated with the MC service group designated as the MC service emergency group.

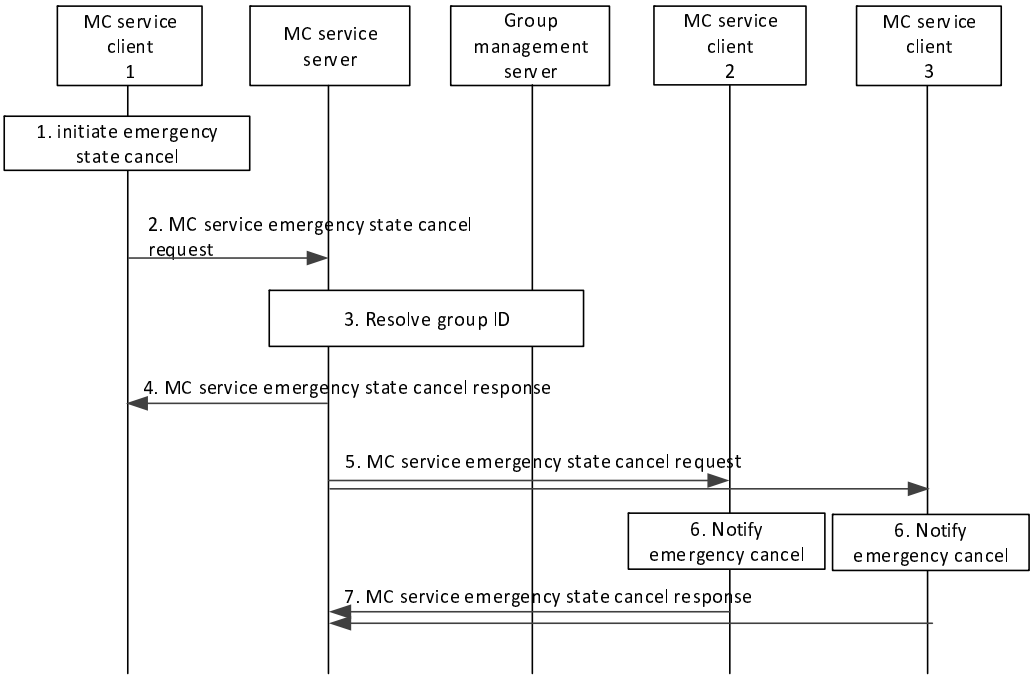

Figure 10.10.1.2.2-1 MC service emergency state cancel

1. The user at the MC service client 1 initiates an MC service emergency state cancel.

NOTE 2: The MC service emergency state cancel request carries an indication to also request that the in-progress emergency is to be cancelled. The MC service 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 MC service client 1. Additionally, an authorized user can cancel either or both the ongoing emergency condition of the group and the initiator's local MC service emergency state.

2. MC service client 1 requests the MC service server to send an MC service emergency state cancel to the MC service group to which MC service client 1 had previously sent the emergency alert.

3. MC service server resolves the MC service group ID to determine the members of that MC service group and their affiliation status, based on the information from group management server.

4. The MC service server sends the MC service emergency state cancel response to the MC service client 1 to confirm the MC service emergency state cancel request. MC service client 1 resets its emergency state.

5. The MC service server sends an MC service emergency state cancel request towards the MC service clients of each of those affiliated MC service group members.

6. MC service users are notified of the MC service emergency state cancellation of MC service client 1.

7. The receiving MC service clients send the MC service emergency state cancel response to the MC service server to acknowledge the MC service emergency state cancel. For a multicast call scenario, these acknowledgements are not sent.

10.10.2 Off-network emergency alert

10.10.2.1 General

The following subclauses specify the procedures for emergency alert initiation and emergency state cancel that are utilised by the following MC services:

- MCVideo service
- MCData service

Editor's note: Whether the following procedures for emergency alert initiation and emergency state cancel apply to MCPTT service also is FFS.

10.10.2.2 MC service emergency alert

10.10.2.2.1 Emergency alert initiation

Figure 10.10.2.2.1-1 describes procedures for the MC service client initiating an MC service emergency alert with an MC service group.

This procedure will place the MC service client in the MC service emergency state if the MC service client is not already in that state.

Pre-conditions:

1. The initiating MC service client 1 has been provisioned with an MC service group designated as the MC service emergency group.

NOTE 1: Alternatively, MC service client 1 could have been provisioned for emergency behaviour on the currently selected group.

2. Information for ProSe direct communications corresponding to the MC service group and its mapping to ProSe Layer-2 Group ID are pre-configured in MC service client 1.
3. MC service client 1 to MC service client N are members of the same MC service group.
4. MC service user 1 has initiated MC service emergency alert.

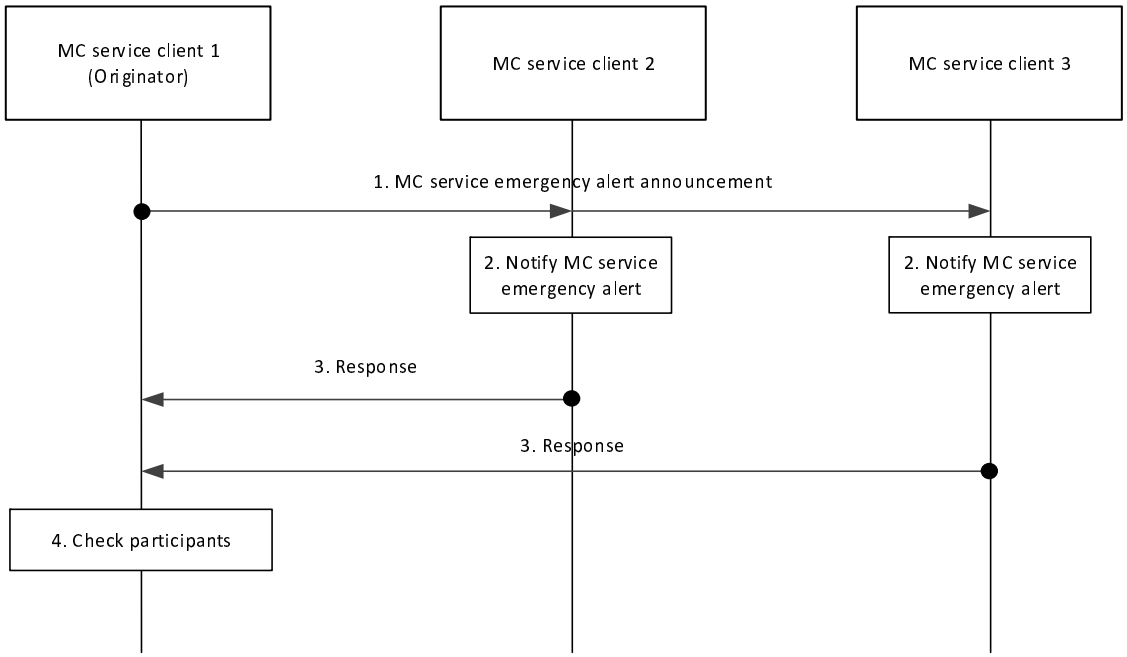

Figure 10.10.2.2.1-1: Emergency alert initiation

1. MC service client 1 sends an MC service emergency alert announcement message to the other clients. MC service client 1 sets its MC service emergency state. This MC service emergency state is retained by the MC service client until explicitly cancelled. Once MC service client1 is in the MC service emergency state, any communications initiated by MC service client 1, group or private, shall be initiated as emergency communications and shall receive priority treatment. The MC service emergency alert announcement is sent periodically so that late joining MC service group members are notified.

NOTE 2: Sending the emergency alert without making a request to also start an MC service emergency communication does not put the group into the in-progress emergency condition.

2. MC service users are notified of the MC service emergency state of the originating MC service user.

3. The MC service clients upon receiving the emergency alert announcement message acknowledge the MC service emergency alert to the originating MC service client.

NOTE 3: The MC service client 1 need not initiate a group communication. For example, the MC service client can be configured to only allow alerts or the MC service user can choose not to make an MC service emergency group communication.

NOTE 4: MC service clients need to respond only to the first emergency alert announcement message that is received.

4. The originating MC service client 1 checks the responses and may inform the MC service user of the MC service group members whose MC service clients responded.

10.10.2.2.2 Emergency state cancel

An MC service client has initiated an MC service emergency alert, has entered the MC service emergency state and wishes to cancel this state, informing the other MC service group members of the cancellation. As part of this process, the MC service client may also request the cancellation of the in-progress emergency condition in the group if authorized to do so.

Procedures in figure 10.10.2.2.2-1 describe procedures for the MC service client cancelling an MC service emergency state.

Pre-conditions:

1. The MC service client 1 has successfully initiated an MC service emergency alert and is in the MC service emergency state.
2. Information for ProSe direct communications corresponding to the MC service group and its mapping to ProSe Layer-2 Group ID are pre-configured in MC service client 1.
3. MC service client 1 to MC service client N are members of the same MC service group.
4. MC service user 1 has initiated MC service emergency alert cancel.

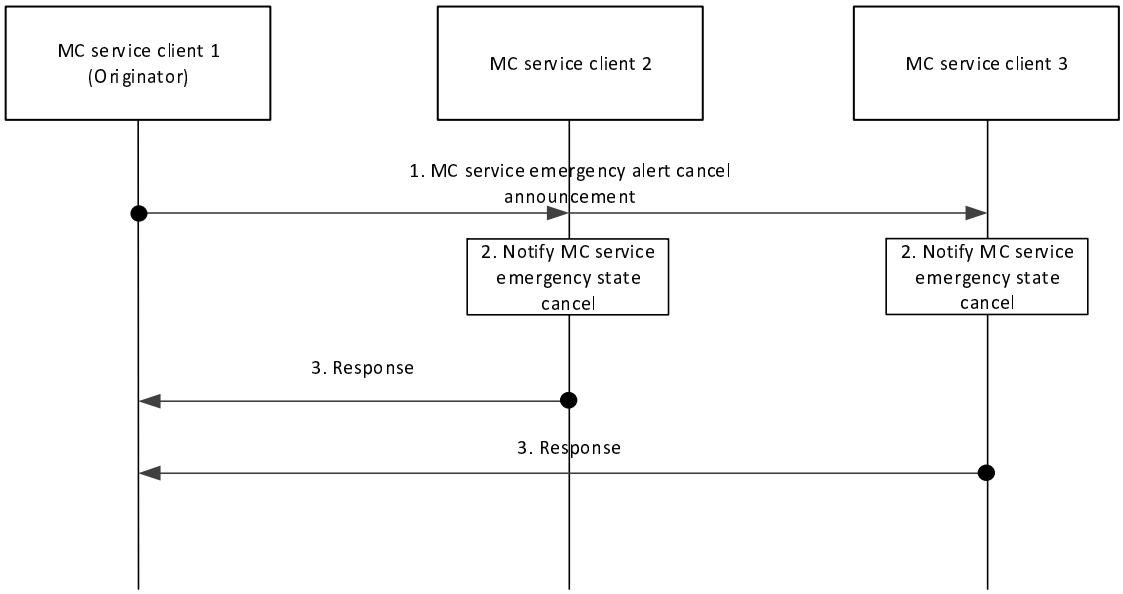

Figure 10.10.2.2.2-1 Emergency state cancel

1. MC service client 1 sends an MC service emergency state cancel announcement to the MC service group to which MC service client 1 had previously sent the emergency alert announcement message.
2. MC service users are notified of the MC service emergency cancellation by MC service client 1.
3. The receiving MC service clients acknowledge the MC service emergency state cancel to the originating MC service client.

NOTE: MC service clients that track the MC service emergency alerts of other MC service users, e.g. clients that fail to receive subsequent periodic MC service emergency alert announcements after a configured timeout can consider the alert to be cancelled.

Annex A (normative): Configuration data for MC services

A.1 General

This Annex provides information about the static data needed for configuration for MC services, which belong to one of the following categories:

- MC service UE configuration data (see subclause A.2);
- MC service user profile data (see subclause A.3);
- MC service group configuration data (see subclause A.4);
- MC service configuration data (see subclause A.5); and
- Initial MC service UE configuration data (see subclause A.6).

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 configuration data in each configuration category corresponds to a single instance of the category type i.e. the MC service UE, MC service group, MC service user and MC service configuration data refers to the information that will be stored against each MC service UE, MC service group, MC service user and MC 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 22.280 [3] or 3GPP TS 22.281 [4] or 3GPP TS 22.282[5] or 3GPP TS 22.179 [2] or the corresponding subclause from the present document.
- Parameter description: A short definition of the semantics of the corresponding item of data, including denotation of the level of the parameter in the configuration hierarchy.
- When it is not clear to which functional entities the parameter is configured, then one or more columns indicating this are provided where the following nomenclature is used:
  - "Y" to denote "Yes" i.e. the parameter denoted for the row needs to be configured to the functional entity denoted for the column.
  - "N" to denote "No" i.e. the parameter denoted for the row does not need to be configured to the functional entity denoted for the column.

Parameters within a set of configuration data have a level within a hierarchy that pertains only to that configuration data. The hierarchy of the configuration data is common across all the three tables of on-network and off-network, on-network only and off-network only. The level of a parameter within the hierarchy of the configuration data is denoted by use of the character ">" in the parameter description field within each table, one per level. Parameters that are at the top-most level within the hierarchy have no ">" character. Parameters that have one or more ">" characters are child parameters of the first parameter above them that has one less ">" character. Parent parameters are parameters that have one or more child parameters. Parent parameters act solely as a "grouping" of their child parameters and therefore do not contain an actual value themselves i.e. they are just containers for their child parameters.

Each parameter that can be configured online shall only be configured through one online reference point. Each parameter that can be configured offline shall only be configured through one offline reference point. The most recent configuration data made available to the MC service UE shall always overwrite previous configuration data, irrespective of whether the configuration data was provided via the online or offline mechanism.

A.2 MC service UE configuration data

MC service UE configuration data has to be known by an MC service UE after MC service authorization. The CSC-4 reference point is used for configuration between the configuration management server and the configuration management client on the MC service UE when the MC service UE is on-network.

MC service UE configuration data can be configured offline using the CSC-11 reference point.

MC service UE configuration data is specific to each MC service and is specified as follows:

- MCPTT UE configuration data is specified in 3GPP TS 23.379 [16];
- MCVideo UE configuration data is specified in 3GPP TS 23.281 [12]; and
- MCData UE configuration data is specified in 3GPP TS 23.282 [13].

Within each MC service, the MC service UE configuration data can be the same or different across MC service UEs.

A.3 MC service user profile configuration data

The MC service user profile configuration data is stored in the MC service user database. The configuration management server is used to configure the MC service user profile configuration data to the MC service user database (CSC-13) and MC service UE (CSC-4).

MC service user profile configuration data can be configured offline using the CSC-11 reference point.

MC service user profile configuration data is specific to each MC service and is specified as follows:

- MCPTT user profile configuration data is specified in 3GPP TS 23.379 [16];
- MCVideo user profile configuration data is specified in 3GPP TS 23.281 [12]; and
- MCData user profile configuration data is specified in 3GPP TS 23.282 [13];

A.4 Group configuration data

The group configuration data is stored in the group management server. The group management server is used to configure the group configuration data to the MC service UE (CSC-2) and the MC service server (CSC-3).

A single group can support one or multiple MC service configurations. Hence, the MC service group configuration data is divided into common group configuration data and MC service specific group configuration data.

The group configuration data can be configured offline using the CSC-12 reference point.

The common group configuration data are specified in table A.4-1. Tables A.4-1 and A.4-2 contain the group configuration required to support the use of on-network MC service. Tables A.4-1 and A.4-3 contain the group configuration required to support the use of off-network MC service.

The MC service related group configuration data specific to each MC service is specified as follows:

- MCPTT related group configuration data is specified in 3GPP TS 23.379 [16];
- MCVideo related group configuration data is specified in 3GPP TS 23.281 [12]; and
- MCData related group configuration data is specified in 3GPP TS 23.282 [13];

Table A.4-1: Common group configuration data (on and off network)

Reference	Parameter description	MC service UE	MC service Server	Group management server
[R-5.17-004], [R-6.4.3-001], [R-6.4.3-002], [R-6.9-004] and [R-5.1.3-002] of 3GPP TS 22.280 [3]	MC service group ID	Y	Y	Y
[R-5.17-004], [R-6.4.3-001], [R-6.4.3-002] and [R-6.9-004] of 3GPP TS 22.280 [3]	Group Alias (Contact URIs)	Y	Y	Y
	List of group members (see NOTE 1)			
[R-5.1.3-001], [R-5.1.5-001], [R-6.4.5-005] and [R-6.4.5-006] of 3GPP TS 22.280 [3]	> MCPTT			
	>> MCPTT ID (see NOTE 2)	N	Y	Y
3GPP TS 33.180 [25]	>> KMSUri for security domain of the MCPTT ID (see NOTE 3)	N	Y	Y
[R-5.1.3-001], [R-5.1.5-001], [R-6.4.5-005] and [R-6.4.5-006] of 3GPP TS 22.280 [3]	> MCVideo			
	>> MCVideo ID (see NOTE 2)	N	Y	Y
3GPP TS 33.180 [25]	>> KMSUri for security domain of the MCVideo ID (see NOTE 3)	N	Y	Y
[R-5.1.3-001], [R-5.1.5-001], [R-6.4.5-005] and [R-6.4.5-006] of 3GPP TS 22.280 [3]	> MCData			
	>> MCData ID (see NOTE 2)	N	Y	Y
3GPP TS 33.180 [25]	>> KMSUri for security domain of the MCData ID (see NOTE 3)	N	Y	Y
[R-6.2.2-001] and [R-7.6-007] of 3GPP TS 22.280 [3]	> User priority for the group	N	Y	Y
[R-5.1.3-001] of 3GPP TS 22.280 [3]	> Participant type for the group (group membership information). The particpant type values are defined and configured by the Mission Critical Organisation (e.g.first responder, second responder, dispatcher, dispatch supervisor, MC service administrator).	N	Y	Y
	> Affiliation status			
	>> MCPTT	N	Y	Y
	>> MCVideo	N	Y	Y
	>> MCData	N	Y	Y
[R-5.16.2-001] and [R-5.16.2-002] of 3GPP TS 22.280 [3]	Group's owner (Mission Critical Organisation)	Y	Y	Y
Subclause 8.3.2, 10.2.3	MC service specific configuration (see NOTE 4)			
	> MCPTT configuration (see NOTE 5)			
	> MCVideo configuration (see NOTE 6)			

	> MCData configuration (see NOTE 7)			
	List of subordinate groups			
[R-5.2.2-002] of 3GPP TS 22.280 [3]	> MC service group ID	N	Y	Y
	Group broadcast information			
[R-5.2.2-001] of 3GPP TS 22.280 [3]	Level within group hierarchy	N	Y	Y
[R-5.2.3-001] of 3GPP TS 22.280 [3]	Level within user hierarchy	N	Y	Y
NOTE 1: The list of group members is provided to an authorized user only upon request and not by default. NOTE 2: MC service IDs for all configured MC services shall be provided for the configured group member. NOTE 3: If this parameter is absent, the KMSUri shall be that identified in the initial MC service UE configuration data (on-network) configured in table A.6-1. NOTE 4: An MC service specific configuration shall be provided for all of the MC services for which the group is enabled. At least one MC service shall be enabled for a group. NOTE 5: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.379 [16]. NOTE 6: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.281 [12]. NOTE 7: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.282 [13].				

Table A.4-2: Common group configuration data (on-network)

Reference	Parameter description	MC service UE	MC service Server	Group management server
[R-6.1-001] of 3GPP TS 22.280 [3]	Maximum number of group members (Nc6)	N	Y	Y
[R-6.1-003] of 3GPP TS 22.280 [3]	Enabled/disabled group (basic status)	Y	Y	Y
[R-6.6.1-006] of 3GPP TS 22.280 [3]	Temporary group indication	Y	Y	Y
[R-6.4.5-005] of 3GPP TS 22.280 [3]	Authorisation to request list of members of an MC service group	Y	Y	Y
	MC service specific configuration			
	> MCPTT configuration (see NOTE 1)			
	> MCVideo configuration (see NOTE 2)			
	> MCData configuration (see NOTE 3)			
[R-6.4.9-006] of 3GPP TS 22.280 [3]	Geographic area within which affiliation to the group is permitted (see NOTE 4)	Y	Y	Y
[R-6.4.9-006] of 3GPP TS 22.280 [3]	Geographic area outside which de-affiliation from the group is mandatory (see NOTE 4)	Y	Y	Y
Subclause 10.2.5	List of authorised users who can retrieve the group information			
	> MCPTT IDs			Y
	> MCVideo IDs			Y
	> MCData IDs			Y
Subclause 5.2.3	Associated relay service code (as specified in 3GPP TS 23.303 [14])	Y	N	Y
NOTE 1: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.379 [16]. NOTE 2: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.281 [12]. NOTE 3: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.282 [13]. NOTE 4: The geographic area may consist of a union of regions that are non-contiguous or contain holes.				

Table A.4-3: Common group configuration data (off-network)

Reference	Parameter description	MC service UE	MC service server	Group management server
Subclause 8.1.3.2	Prose layer-2 group ID (as specified in 3GPP TS 23.303 [14])	Y	N	Y
Subclause 8.1.3.2	ProSe group IP multicast address (as specified in 3GPP TS 23.303 [14])	Y	N	Y
Subclause 8.1.3.2	Indication of whether the UE shall use IPv4 or IPv6 for the MC service group (as specified in 3GPP TS 23.303 [14])	Y	N	Y
	MC service specific configuration			
	> MCPTT configuration (see NOTE 1)			
	> MCVideo configuration (see NOTE 2)			
	> MCData configuration (see NOTE 3)			
NOTE 1: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.379 [16]. NOTE 2: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.281 [12]. NOTE 3: This parameter is a parent parameter whose child parameters are defined in 3GPP TS 23.282 [13].				

A.5 MC service configuration data

The MC service configuration data is stored in the MC service server. The configuration management server is used to configure the MC service configuration data to the MC service server (CSC-5) and the MC service UE (CSC-4).

The MC service configuration data can be configured offline using the CSC-11 reference point.

The MC service configuration data is specific to each MC service and hence the detailed list of MC service configuration data is listed as follows:

- MCPTT service configuration data is specified in 3GPP TS 23.379 [16];
- MCVideo service configuration data is specified in 3GPP TS 23.281 [12]; and
- MCData service configuration data is specified in 3GPP TS 23.282 [13];

A.6 Initial MC service UE configuration data

The initial MC service UE configuration data is essential to the MC service UE to successfully connect to the MC system. The initial MC service UE configuration data can be the same or different across MC service UEs.

Data in table A.6-1 is provided to the MC service UE's clients (e.g. MC service client, group management client, configuration management client, identity management client, key management client) during the bootstrap process (see subclause 10.1.1), and can be configured on the MC service UE offline using the CSC-11 reference point or via other means e.g. as part of the MCPTT client's provisioning on the UE, using a device management procedure.

Table A.6-1: Initial MC service UE configuration data (on-network)

Reference	Parameter description
Subclause 10.1.1	PDN connectivity information
	> HPLMN ID and optionally VPLMN ID to which the data pertains
	> MC services PDN
	>> APN
	>> PDN access credentials
	> MC common core services PDN
	>> APN
	>> PDN access credentials
	> MC identity management service PDN
	>> APN
	>> PDN access credentials
Subclause 10.1.1	Application plane server identity information
	> Identity management server
	>> Server URI
	> Configuration management server
	>> Server URI
	> Key management server
	>> Server URI
	>> KMSUri for security domain managed by KMS

Annex B (informative): Service continuity for MC service

B.1 Service continuity between on-network MC service and UE-to-network relay MC service

This annex describes how 3GPP TS 23.237 [10] mechanisms for IMS service continuity can be used to provide service continuity between on-network MC service and UE-to-network relay MC service. For illustration, MCPTT AS is considered as the MC service.

Only the procedure for service continuity from on-network MCPTT service to UE-to-network relay MCPTT service is described in figure B.1-1. The procedure for service continuity in the opposite direction is identical.

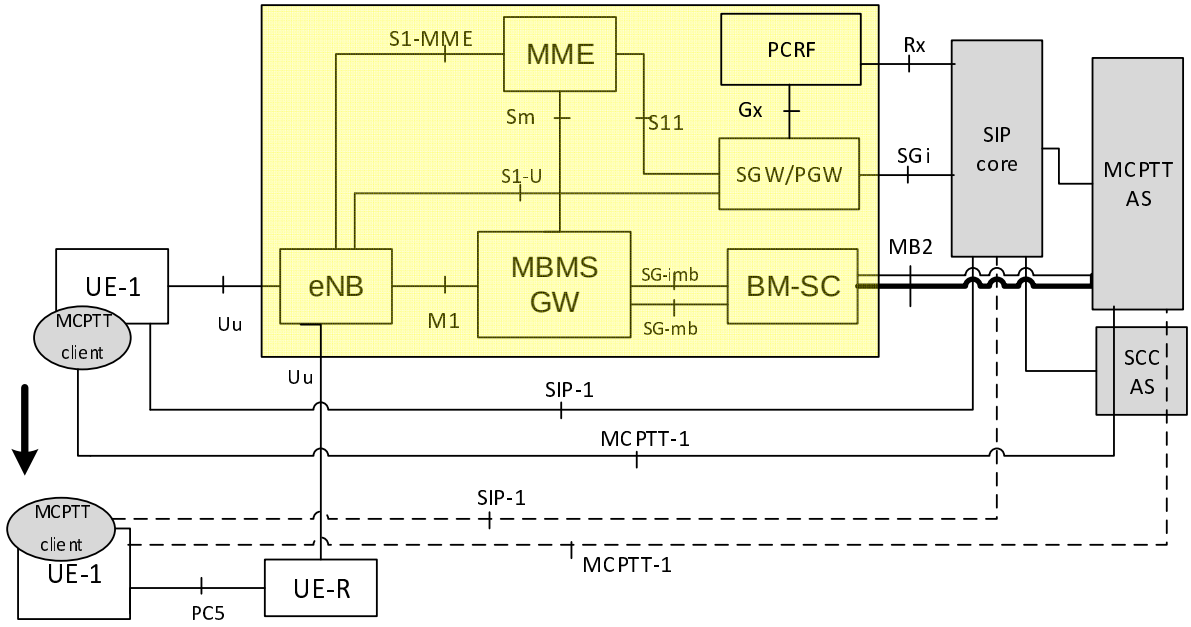

Figure B.1-1: Service continuity from on-network to UE-to-network relay

As illustrated in figure B.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 B.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 B.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 [10].

Depicted in figure B.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.

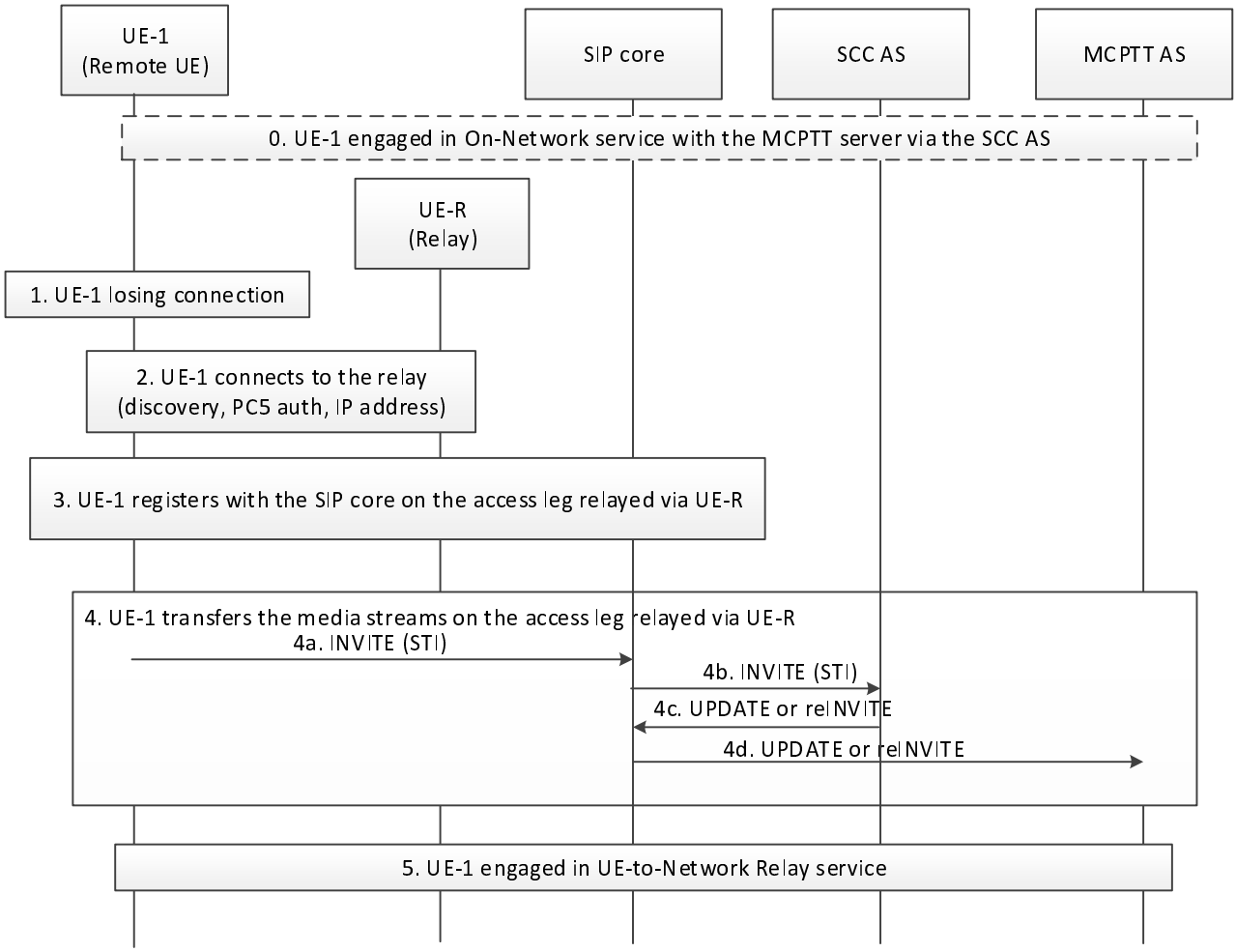

Figure B.1-2 Service continuity when UE switches from on-network MCPTT service to UE-to-network relay MCPTT service

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 [10].

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 [14]. 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 [14].

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 C (informative): Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2016-04						Initial version.	0.0.0
2016-04						Alignment with the following Rel-13 CRs agreed at SA6#10: CR0057(S6-160312), CR0063(S6-160189), CR0065(S6-160362),CR0068(S6-160348), CR0069(S6-160313), CR0070(S6-160280), CR0071(S6-160199), CR0079(S6-160360), CR0080(S6-160297), CR0085(S6-160361), CR0092(S6-160345), CR0095(S6-160339), CR0099(S6-160342)	0.1.0
2016-06						Implemented the following pCRs approved in SA6#11: S6-160378, S6-160489, S6-160492, S6-160504, S6-160524, S6-160528, S6-160560, S6-160561, S6-160570, S6-160578, S6-160579, S6-160583, S6-160600, S6-160601 Also implemented the Rapporteur actions from SA6#11: 1. Removed all colour coding from the TS 2. Fixed the subclauses numbering in the entire TS. 3. Generalized the text as per agreed terminology. 4. Added references for TS 23.303 and TS 23.237	0.2.0
2016-08						Implemented the following pCRs approved in SA6#12: S6-160794, S6-160795, S6-160796, S6-160797, S6-160798, S6-160799, S6-160880, S6-160888, S6-160919, S6-160920	0.3.0
2016-09						Implemented the pCR S6-160822 which was approved in SA6#12 Modified the references order	0.4.0
2016-10						Implemented the following pCRs approved in SA6#13: S6-160960, S6-161119, S6-161120, S6-161122, S6-161128, S6-161207, S6-161208, S6-161214, S6-161215, S6-161220, S6-161252, S6-161255	0.5.0
2016-11						Implemented the following pCRs approved in SA6#14: S6-161417, S6-161490, S6-161521, S6-161527, S6-161530, S6-161531, S6-161539, S6-161571, S6-161582, S6-161583, S6-161592, S6-161593, S6-161606, S6-161617, S6-161618, S6-161619, S6-161620, S6-161625, S6-161627, S6-161632, S6-161638	0.6.0
2016-11	SA#74	SP-160875				Submitted for Approval at SA#74	1.0.0
2016-12	SA#74	SP-160875				MCC Editorial update for publication after TSG SA approval (SA#74)	14.0.0
2017-03	SA#75	SP-170069	0001	1	F	Alignment of definitions	14.1.0
2017-03	SA#75	SP-170069	0002	2	F	Alignment of group affiliation and de-affiliation requirements	14.1.0
2017-03	SA#75	SP-170069	0003	1	F	Alignment of bearer management	14.1.0
2017-03	SA#75	SP-170068	0004	1	F	Removal of CSC-6 from figure 7.3.1-1	14.1.0
2017-03	SA#75	SP-170069	0005	1	F	CFA Correction of information flow for MBMS	14.1.0
2017-03	SA#75	SP-170069	0009	1	F	Corrections on group configuration tables	14.1.0
2017-03	SA#75	SP-170069	0012	1	F	MBMS quality report clarifications	14.1.0
2017-03	SA#75	SP-170069	0014	2	D	Resolving editor's note on service continuity	14.1.0
2017-03	SA#75	SP-170069	0015	2	F	Clarification on Editor's notes in CFA	14.1.0
2017-03	SA#75	SP-170069	0020	3	F	Add location management entities and reference points in figure 7.3.1-3	14.1.0
2017-03	SA#75	SP-170069	0022	1	F	Clarification that initial UE config and UE config are specific to one or more UEs	14.1.0
2017-03	SA#75	SP-170069	0023	1	F	Identities used in location information procedures	14.1.0
2017-06	SA#76	SP-170390	0024	1	F	Correction on Annex A Configuration data for MC services	14.2.0
2017-06	SA#76	SP-170390	0033	1	F	Addition of MC service to group configuration request	14.2.0

2017-06	SA#76	SP-170390	0034		F	Miscellaneous corrections to configuration	14.2.0
2017-06	SA#76	SP-170390	0035	2	F	Corrections on determination of MBMS bearer quality	14.2.0
2017-06	SA#76	SP-170390	0044	1	F	Add note to bearer coordination procedure	14.2.0
2017-06	SA#76	SP-170390	0050		F	Correction of information flow MBMS listening report	14.2.0
2017-06	SA#76	SP-170390	0054	1	F	Alignment of server address with stage 3	14.2.0
2017-06	SA#76	SP-170390	0055	2	F	Inclusion of KMSUri to allow multiple security domains	14.2.0
2017-06	SA#76	SP-170390	0063	1	F	Corrections to Group configuration data for all MC services	14.2.0

History

Document history		
V14.1.0	May 2017	Publication
V14.2.0	July 2017	Publication